EXHIBIT 2

Table of Contents

As filed with the Securities and Exchange Commission on May 14, 2021

Registration No. 333-

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM S-4
REGISTRATION STATEMENT

UNDER

THE SECURITIES ACT OF 1933

LGL SYSTEMS ACQUISITION CORP.

(Exact name of Registrant as specified in its charter)

Delaware	7372	83-4599446
(State or other jurisdiction of incorporation or organization)	(Primary standard industrial classification code number)	(I.R.S. Employer Identification Number)

165 W. Liberty Street, Suite 220
Reno, NV 89501
Telephone: (705) 393-9113
(Address, including zip code, and telephone number, including area code, of registrant's principal executive offices)

Robert LaPenta Jr.
Co-Chief Executive Officer
LGL Systems Acquisition Corp.
165 W. Liberty Street, Suite 220
Reno, NV 89501
Telephone: (705) 393-9113
(Name, address, including zip code, and telephone number, including area code, of agent for service)

With copies to:

Michael L. Zuppone Luke P. Iovine, III Keith D. Pisani Paul Hastings LLP 200 Park Avenue New York, NY 10166 (212) 318-6000	Brian F. Leaf Garth A. Osterman Cooley LLP One Freedom Square RestonTown Center 11951 Freedom Drive Reston, VA 20190 (703) 456-8000

Approximate date of commencement of proposed sale of the securities to the public: As soon as practicable after this Registration Statement becomes effective and all other conditions to the transactions contemplated by the Agreement and Plan of Reorganization and Merger described in the included proxy statement/prospectus have been satisfied or waived.

If the securities being registered on this form are to be offered in connection with the formation of a holding company and there is compliance with General Instruction G, check the following box: ☐

If this form is filed to register additional securities for an offering pursuant to Rule 462(b) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this form is a post-effective amendment filed pursuant to Rule 462(d) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☐	Accelerated filer	☐
Non-accelerated filer	☒	Smaller reporting company	☒
		Emerging growth company	☒

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 7(a)(2)(B) of the Securities Act. ☐

If applicable, place an X in the box to designate the appropriate rule provision relied upon in conducting this transaction:

Exchange Act Rule 13e-4(i) (Cross-Border Issuer Tender Offer) ☐

Exchange Act Rule 14d-1(d) (Cross-Border Third-Party Tender Offer) ☐

CALCULATION OF REGISTRATION FEE

Title of Each Class of Security To Be Registered	Amount To Be Registered(1)	Proposed Maximum Offering Price Per Security	Proposed Maximum Aggregate Offering Price(2)	Amount of Registration Fee(3)
Common Stock, par value $0.0001 per share(1)	86,340,000	N/A	$3,563.82	$0.39

(1) Represents shares of common stock to be issued by the registrant to the securityholders of IronNet Cybersecurity, Inc. ("*IronNet*") in connection with the Business Combination described herein.

(2) Estimated solely for the purpose of calculating the registration fee in accordance with Rule 457(f)(2) of the Securities Act of 1933, as amended. IronNet is a private company, no market exists for its securities, and IronNet has an accumulated deficit. Therefore, the proposed maximum aggregate offering price is one-third of the aggregate par value of the IronNet securities expected to be exchanged in the Merger, including IronNet securities issuable upon the exercise of options or settlement of restricted stock units.

(3) Calculated pursuant to Rule 457 of the Securities Act by calculating the product of (i) the proposed maximum aggregate offering price and (ii) 0.0001091.

The registrant hereby amends this registration statement on such date or dates as may be necessary to delay its effective date until the registrant shall file a further amendment which specifically states that this registration statement shall thereafter become effective in accordance with Section 8(a) of the Securities Act of 1933, as amended, or until the registration statement shall become effective on such date as the Securities and Exchange Commission, acting pursuant to said Section 8(a), may determine.

Table of Contents

PRELIMINARY PROXY STATEMENT
SUBJECT TO COMPLETION, DATED MAY 14, 2021

LGL SYSTEMS ACQUISITION CORP.
165 W. Liberty Street, Suite 220
Reno, NV 89501

NOTICE OF
SPECIAL MEETING
TO BE HELD ON , 2021

TO THE STOCKHOLDERS OF LGL SYSTEMS ACQUISITION CORP.:

NOTICE IS HEREBY GIVEN that a special meeting of LGL Systems Acquisition Corp. ("*LGL*"), a Delaware corporation, will be held at :00 a.m. Eastern Time, on , 2021, in a virtual format. You are cordially invited to attend the special meeting, which will be held for the following purposes:

(1) **Proposal No. 1—The Business Combination Proposal**—to consider and vote upon a proposal to approve and adopt the Agreement and Plan of Reorganization and Merger, dated as of March 15, 2021 (as may from time to time be amended, restated, supplemented or otherwise modified, the "*Merger Agreement*"), by and among LGL, LGL Systems Merger Sub Inc., a Delaware corporation and wholly owned subsidiary of LGL ("*Merger Sub*"), and IronNet Cybersecurity, Inc., a Delaware corporation ("*IronNet*"), a copy of which is attached to this proxy statement/prospectus as *Annex A*, and the transactions contemplated thereby, including the merger of Merger Sub with and into IronNet, with IronNet surviving as a wholly owned subsidiary of LGL (the "*Business Combination*", and LGL post-Business Combination being referred to as "*LGL*" or the "*Combined Company*") —we refer to this proposal as the "*Business Combination proposal*";

(2) **Proposal No. 2—The LGL Charter Proposals**—to consider and vote upon separate proposals to approve amendments to LGL's current amended and restated certificate of incorporation (the "*Existing Certificate*"). The proposed amendments detailed below will be voted on separately and are collectively referred to as the "*LGL charter proposals*":

(i) *Name Change Charter Amendment*—to change the name of the public entity to "IronNet, Inc." as opposed to "LGL Systems Acquisition Corp.";

(ii) *Authorized Share Charter Amendment*—to increase LGL's capitalization so that it will have 500,000,000 authorized shares of a single class of common stock and 100,000,000 authorized shares of preferred stock, as opposed to LGL having 75,000,000 authorized shares of Class A common stock, 10,000,000 authorized shares of Class B common stock and 1,000,000 authorized shares of preferred stock;

(iii) *Actions by Stockholders Charter Amendment*—to require that stockholders only act at annual and special meeting of the corporation and not by written consent;

(iv) *Corporate Opportunity Charter Amendment*—to eliminate the current limitations in place on the corporate opportunity doctrine;

(v) *Voting Thresholds Charter Amendment*—to increase the required vote thresholds to 66 2/3% for stockholders to approve amendments to the bylaws and amendments to certain provisions of the certificate of incorporation; and

(vi) *Additional Charter Amendment*—to approve all other changes, including to delete the various provisions applicable only to special purpose acquisition corporations (such as the obligation to dissolve and liquidate if a business combination is not consummated within a certain period of time) that will no longer be relevant following the consummation of the Business Combination (the "*closing*");

(3) **Proposal No. 3—The NYSE Proposal**—to consider and vote upon a proposal to approve, for purposes of complying with applicable listing rules of The NYSE (the "*NYSE*"), the issuance of shares of common stock pursuant to the Business Combination and the issuance of shares of common stock to certain accredited investors or qualified institutional buyers in a private placement, the proceeds of which will be used to finance the Business Combination and related transactions and the costs and expenses incurred in connection therewith with any balance used for working capital purposes—we refer to this proposal as the "*NYSE proposal*";

(4) **Proposal No. 4—The Director Election Proposal**—to consider and vote upon a proposal to elect eleven (11) directors who, upon consummation of the Business Combination, will become the directors of the Combined Company—we refer to this proposal as the "*director election proposal*";

(5) **Proposal No. 5—The Incentive Plan Proposal**—to consider and vote upon a proposal to approve the IronNet, Inc. 2021 Equity Incentive Plan, which is an incentive compensation plan for directors and employees of the Combined Company following the Business Combination —we refer to this proposal as the "*incentive plan proposal*";

(6) **Proposal No. 6 —The ESPP Proposal—** to consider and vote upon a proposal to approve the IronNet, Inc. 2021 Employee Stock Purchase Plan (the "*ESPP*"), to assist the Combined Company in aligning the long-term financial interests of its employees with the financial interests of its stockholders, as well as attracting, retaining and motivating employees and encouraging them to devote their best efforts to the Combined Company's business and financial success—we refer to this proposal as the "*ESPP proposal*";

(7) **Proposal No. 7—The Adjournment Proposal**—to consider and vote upon a proposal to adjourn the special meeting to a later date or dates if it is determined that more time is necessary or appropriate, in the judgment of LGL's board of directors or the officer presiding over the special meeting, for LGL to consummate the Business Combination (including to solicit additional votes in favor of any of the foregoing proposals)—we refer to this proposal as the "*adjournment proposal*."

These items of business are described in the attached proxy statement/prospectus. **We encourage you to read the attached proxy statement/prospectus in its entirety, including the Annexes and accompanying financial statements, before voting. IN PARTICULAR, WE URGE YOU TO CAREFULLY READ THE SECTION ENTITLED "*RISK FACTORS.*"**

Only holders of record of LGL common stock at the close of business on , 2021 (the "*LGL Record Date*") are entitled to notice of the special meeting and to vote and have their votes counted at the special meeting and any adjournments or postponements of the special meeting. LGL stockholders may attend, vote and examine the list of LGL stockholders entitled to vote at the special meeting by visiting and entering the control number found on their proxy card, voting instruction form or notice they receive.

After careful consideration, LGL's board of directors has determined that each of the Business Combination proposal, the LGL charter proposals, the NYSE proposal, the director election proposal, the incentive plan proposal, the ESPP proposal and the adjournment proposal is fair to and in the best interests of LGL and its stockholders and unanimously recommends that you vote or give instruction to vote "FOR" the Business Combination proposal, "FOR" each of the LGL charter proposals, "FOR" the NYSE proposal, "FOR" the election of all of the persons nominated by LGL's management for election as directors, "FOR" the incentive plan proposal, "FOR" the ESPP proposal and "FOR" the adjournment proposal, if presented. When you consider the recommendation of LGL's board of directors, you should keep in mind that LGL's directors and officers may have interests in the Business Combination that conflict with your interests as a stockholder. See the section entitled "*Proposal No. 1—The Business Combination Proposal—Interests of the Sponsor and LGL's Directors and Officers in the Business Combination*."

Pursuant to the Existing Certificate, LGL is providing the holders of shares of LGL Class A common stock originally sold as part of the units issued in its initial public offering (the "*IPO*," such shares, the "*Public Shares*," and such holders, the "*Public Stockholders*") with the opportunity to redeem, upon the closing, the

Public Shares then held by them for cash equal to their pro rata share of the aggregate amount on deposit as of two business days prior to the closing, in the trust account (the "*Trust Account*") that holds the proceeds (including interest not previously released to LGL to pay its income taxes or any other taxes payable) from the IPO. For illustrative purposes, based on the fair value of cash and marketable securities held in the Trust Account as of , 2021, the LGL Record Date, of approximately $ million, the estimated per share redemption price would have been approximately $. Public stockholders may elect to redeem their shares whether or not they are holders as of the LGL Record Date and whether or not they vote for the Business Combination proposal. Holders of LGL's outstanding warrants sold in the IPO, which are exercisable for shares of LGL common stock under certain circumstances, do not have redemption rights in connection with the Business Combination. LGL Systems Acquisition Holding Company, LLC, as the initial stockholder of LGL (the "*Sponsor*") has agreed to waive its redemption rights in connection with the Closing with respect to its shares, and the Sponsor's shares will be excluded from the pro rata calculation used to determine the per share redemption price. As of the LGL Record Date, the Sponsor owned approximately % of outstanding LGL common stock.

Consummation of the Business Combination is conditioned on approval of the Business Combination proposal, the LGL charter proposals, the NYSE proposal and the director election proposal (and each such proposal is cross-conditioned on the approval of each such other proposal) (collectively, the "*Required Proposals*"). The incentive plan proposal and ESPP proposal are conditioned upon the approval of the Required Proposals. If any of the Required Proposals is not approved, the other proposals will not be presented to LGL stockholders for a vote.

All LGL stockholders are cordially invited to attend the special meeting which will be held in virtual format. You will not be able to physically attend the special meeting. To ensure your representation at the special meeting, however, you are urged to complete, sign, date and return the proxy card accompanying the proxy statement/prospectus as soon as possible. If you are a stockholder of record holding shares of LGL common stock, you may also cast your vote at the special meeting electronically by visiting . If your shares are held in an account at a brokerage firm or bank, you must instruct your broker or bank on how to vote your shares or, if you wish to attend the special meeting and vote electronically, obtain a proxy from your broker or bank.

A complete list of LGL stockholders of record entitled to vote at the special meeting will be available for ten days before the special meeting at the principal executive offices of LGL for inspection by stockholders during business hours for any purpose germane to the special meeting.

Your vote is important regardless of the number of shares you own. **Whether you plan to attend the special meeting or not, please complete, sign, date and return the enclosed proxy card as soon as possible in the envelope provided. If your shares are held in "street name" or are in a margin or similar account, you should contact your broker to ensure that votes related to the shares you beneficially own are properly counted.**

Thank you for your participation. We look forward to your continued support.

By Order of the Board of Directors

Marc J. Gabelli
Chairman of the Board of Directors and Co-Chief Executive Officer

, 2021

IF YOU RETURN YOUR PROXY CARD WITHOUT AN INDICATION OF HOW YOU WISH TO VOTE, YOUR SHARES WILL BE VOTED IN FAVOR OF EACH OF THE PROPOSALS.

ALL LGL PUBLIC STOCKHOLDERS HAVE THE RIGHT TO HAVE THEIR SHARES REDEEMED FOR CASH IN CONNECTION WITH THE PROPOSED BUSINESS COMBINATION. PUBLIC STOCKHOLDERS ARE NOT REQUIRED TO AFFIRMATIVELY VOTE FOR OR AGAINST THE BUSINESS COMBINATION PROPOSAL OR BE HOLDERS OF RECORD ON THE RECORD DATE IN ORDER TO HAVE THEIR SHARES REDEEMED FOR CASH. THIS MEANS THAT ANY PUBLIC STOCKHOLDER HOLDING SHARES OF LGL COMMON STOCK MAY EXERCISE REDEMPTION RIGHTS REGARDLESS OF WHETHER THEY ARE EVEN ENTITLED TO VOTE ON THE BUSINESS COMBINATION PROPOSAL.

TO EXERCISE REDEMPTION RIGHTS, HOLDERS MUST TENDER THEIR STOCK TO CONTINENTAL STOCK TRANSFER & TRUST COMPANY, LGL'S TRANSFER AGENT, NO LATER THAN TWO BUSINESS DAYS PRIOR TO THE SPECIAL MEETING. YOU MAY TENDER YOUR STOCK EITHER BY DELIVERING YOUR STOCK CERTIFICATE TO THE TRANSFER AGENT OR BY DELIVERING YOUR SHARES ELECTRONICALLY USING THE DEPOSITORY TRUST COMPANY'S DEPOSIT WITHDRAWAL AT CUSTODIAN SYSTEM. IF THE BUSINESS COMBINATION IS NOT COMPLETED, THEN THESE SHARES WILL NOT BE REDEEMED FOR CASH. IF YOU HOLD THE SHARES IN "STREET NAME," YOU WILL NEED TO INSTRUCT THE ACCOUNT EXECUTIVE AT YOUR BANK OR BROKER TO WITHDRAW THE SHARES FROM YOUR ACCOUNT IN ORDER TO EXERCISE YOUR REDEMPTION RIGHTS. SEE THE SECTION ENTITLED "*SPECIAL MEETING OF LGL STOCKHOLDERS—REDEMPTION RIGHTS*" FOR MORE SPECIFIC INSTRUCTIONS.

Table of Contents

The information in this proxy statement/prospectus is not complete and may be changed. We may not issue these securities until the registration statement filed with the Securities and Exchange Commission is effective. This proxy statement/prospectus is not an offer to sell these securities, and it is not soliciting an offer to buy these securities in any jurisdiction where the offer or sale is not permitted.

SUBJECT TO COMPLETION, DATED MAY 14, 2021

PROXY STATEMENT FOR SPECIAL MEETING OF

LGL SYSTEMS ACQUISITION CORP.

PROSPECTUS FOR UP TO SHARES OF COMMON STOCK

The board of directors of each of LGL Systems Acquisition Corp., a Delaware corporation ("*LGL*"), and IronNet Cybersecurity, Inc., a Delaware corporation ("*IronNet*"), has unanimously approved the Agreement and Plan of Reorganization and Merger, dated as of March 15, 2021 (as may from time to time be amended, restated, supplemented or otherwise modified, the "*Merger Agreement*"), by and among LGL, LGL Systems Merger Sub Inc., a Delaware corporation and wholly owned subsidiary of LGL ("*Merger Sub*"), and IronNet, pursuant to which Merger Sub will merge with and into IronNet, with IronNet surviving as a wholly owned subsidiary of LGL (the "*Business Combination*", and the post-Business Combination entity being referred to as "*LGL*" or the "*Combined Company*"). Upon the closing of the Business Combination, LGL intends to change its name from "LGL Systems Acquisition Corp." to "IronNet, Inc."

Pursuant to the Merger Agreement, (i) each outstanding share of IronNet common stock and IronNet preferred stock (with each share of IronNet preferred stock being treated as if it were converted into ten (10) shares of IronNet common stock on the effective date of the Business Combination) will be converted into the right to receive (a) a number of shares of LGL common stock equal to the exchange ratio, the numerator of which is $863,400,000 divided by $10.00, and the denominator of which is equal to the number of shares of IronNet common stock on a fully-diluted basis as of immediately prior to the effective time of the Business Combination, including shares of IronNet common stock issuable upon conversion/exercise of outstanding IronNet options, IronNet warrants, IronNet restricted stock units and IronNet restricted stock awards (in each case, whether or not vested) and (b) a cash amount payable in respect of fractional shares of LGL common stock that would otherwise be issued in connection with the foregoing conversion, if applicable, and (ii) each IronNet option, IronNet restricted stock unit, IronNet restricted stock award or IronNet warrant that is outstanding immediately prior to the closing of the transactions (and by its terms will not terminate upon the closing of the transactions) will remain outstanding and thereafter (x) in the case of options, represent the right to purchase a number of shares of LGL common stock equal to the number of shares of IronNet common stock subject to such option multiplied by the same exchange ratio used for IronNet common stock (rounded down to the nearest whole share) at an exercise price per share equal to the current exercise price per share for such option divided by such exchange ratio (rounded up to the nearest whole cent), (y) in the case of warrants, represent the right to purchase a number of shares of LGL common stock equal to the number of shares of IronNet preferred stock subject to such warrant multiplied by such exchange ratio, multiplied by ten (10) at an exercise price equal to the current exercise price per share (rounded up to the nearest whole cent) for such warrant divided by such exchange ratio, divided by ten (10) (rounded down to the nearest whole share), and (z) in the case of stock units and restricted stock awards, represent a number of shares of LGL common stock equal to the number of shares of IronNet common stock subject to such stock unit or restricted stock award multiplied by such exchange ratio (rounded down to the nearest whole share). In addition, IronNet stockholders and eligible holders of options, warrants, restricted stock unit awards and restricted stock awards (as applicable, only to the extent time vested as of the closing of the Business Combination) may also receive as additional merger consideration a pro rata portion of 1,078,125 additional shares of LGL common stock if the volume weighted average share price for LGL's common stock equals or exceeds $13.00 for ten (10) consecutive days during the two year period following the closing of the Business Combination (the "*Earnout Shares*").

If calculated based on the capitalization of IronNet as of March 15, 2021, the exchange ratio is approximately 0.8076 of a share of LGL common stock per fully-diluted share of IronNet common stock.

Proposals to approve and adopt the Merger Agreement and the other matters discussed in this proxy statement/prospectus will be presented for approval by LGL stockholders at the special meeting of stockholders of LGL scheduled to be held on , 2021, in virtual format and approval by IronNet stockholders via written consent.

On March 15, 2021, LGL executed subscription agreements with certain investors for the sale of an aggregate of 12,500,000 shares of LGL common stock in a private placement transaction at a purchase price of $10.00 per share for aggregate gross cash proceeds of $125 million. The closing of the sale of these shares will occur concurrently with the consummation of the Business Combination. Of the amounts subscribed for in the private placement, the Sponsor has agreed to purchase 566,000 shares of Class A common stock for $5,660,000.

LGL's Class A common stock, redeemable warrants exercisable for shares of Class A common stock at an exercise price of $11.50 per share, and units (each consisting of one share of Class A common stock and one-half of one redeemable warrant), are currently listed on the New York Stock Exchange (the "*NYSE*") under the symbols DFNS, DFNS.WS and DFNS.U, respectively. Upon the closing of the Business Combination, it is contemplated that LGL will have a single class of common stock. LGL intends to apply for listing on the NYSE, to be effective at the consummation of the Business Combination, of the common stock to be issued in connection with the Business Combination (including the common stock issued pursuant to the related private placement) together with the common stock previously issued in its initial public offering, the warrants issued in its initial public offering and simultaneous private placement, and the common stock underlying the warrants issued in its initial public offering and simultaneous private placement, under the proposed symbols IRNT, in the case of the common stock, and IRNT.WS, in the case of the warrants. LGL will not have units traded on the NYSE following consummation of the Business Combination. It is a condition of the consummation of the Business Combination that the LGL common stock is approved for listing on the NYSE (subject only to official notice of issuance thereof and public holder requirements), but there can be no assurance such listing condition will be met. If such listing condition is not met, the Business Combination will not be consummated unless the listing condition set forth in the Merger Agreement is waived by the parties to that agreement.

LGL is an "emerging growth company" as defined in the Jumpstart Our Business Startups Act of 2012, as amended (the "*JOBS Act*"), and has elected to comply with certain reduced public company reporting requirements.

This proxy statement/prospectus provides you with detailed information about the Business Combination and other matters to be considered at the special meeting of LGL stockholders and by IronNet stockholders. We encourage you to carefully read this entire document. **You should also carefully consider the risk factors described in the section entitled "*Risk Factors*" beginning on page 34. These securities have not been approved or disapproved by the Securities and Exchange Commission or any state securities commission nor has the Securities and Exchange Commission or any state securities commission passed upon the accuracy or adequacy of this proxy statement/prospectus. Any representation to the contrary is a criminal offense.**

This proxy statement/prospectus is dated , 2021, and is first being mailed to LGL stockholders on or about such date.

IMPORTANT NOTE ABOUT THIS PROXY STATEMENT/ PROSPECTUS

This document, which forms part of a registration statement on Form S-4 filed with the SEC by LGL (File No. 333-) (the "Registration Statement"), constitutes a prospectus of LGL under Section 5 of the Securities Act, with respect to the shares of LGL common stock to be issued if the Business Combination described herein is consummated. This document also constitutes a notice of meeting and a proxy statement/prospectus under Section 14(a) of the Exchange Act with respect to the special meeting of LGL stockholders at which LGL stockholders will be asked to consider and vote upon a proposal to approve the Business Combination by the approval and adoption of the Merger Agreement, among other matters.

You should rely only on the information contained in this proxy statement/prospectus in determining whether to vote in favor of the Business Combination and the other proposals. No one has been authorized to provide you with information that is different from that contained in this proxy statement/prospectus. This proxy statement/prospectus is dated , 2021. You should not assume that the information contained in this proxy statement/prospectus is accurate as of any date other than that date. Neither the mailing of this proxy statement/prospectus to LGL stockholders or IronNet stockholders nor the issuance by LGL of common stock in connection with the Business Combination will create any implication to the contrary.

SUMMARY OF THE MATERIAL TERMS OF THE BUSINESS COMBINATION

- The parties to the Business Combination are LGL, Merger Sub and IronNet. Pursuant to the Merger Agreement, Merger Sub will merge with and into IronNet, with IronNet surviving as a wholly owned subsidiary of LGL. See the section entitled "*The Merger Agreement*."
- Pursuant to the Merger Agreement, (i) if the Exchange Ratio were calculated based on capitalization of IronNet as of March 15, 2021, each outstanding share of IronNet common stock and IronNet preferred stock (with each share of IronNet preferred stock being treated as if it were converted into ten (10) shares of IronNet common stock on the effective date of the Business Combination) will be converted into the right to receive approximately 0.8076 of a share of LGL common stock, and (ii) each IronNet option, IronNet restricted stock unit, IronNet restricted stock award or IronNet warrant that is outstanding immediately prior to the closing of the transactions (and by its terms will not terminate upon the closing of the transactions) will remain outstanding and will be exercisable for or represent an underlying number of shares of LGL common stock correspondingly adjusted by the Exchange Ratio. IronNet stockholders and eligible holders of options, warrants, restricted stock unit awards and restricted stock awards (as applicable, only to the extent time vested as of the closing of the Business Combination) may also receive as additional merger consideration a pro rata portion of 1,078,125 shares of LGL common stock if the volume weighted average share price for LGL's common stock equals or exceeds $13.00 for ten (10) consecutive trading days during the two year period following the closing of the Business Combination. See the section entitled "*Proposal No. 1—The Business Combination Proposal—Structure of the Transactions.*"
- Immediately following the closing of the Business Combination, IronNet stockholders will hold approximately 72.3% of the issued and outstanding Combined Company Common Stock (on account of Combined Company Common Stock issued in the Business Combination), current LGL Public Stockholders will hold approximately 14.5% of the issued and outstanding Combined Company Common Stock, the Sponsor will hold approximately 3.2% of the Combined Company Common Stock and the remaining 10.0% will be held by the Subscription Investors (other than the Sponsor) purchasing LGL common stock in the Private Placement (defined below), in each case, based on the number of shares of LGL common stock outstanding as of December 31, 2020 (assuming no holder of LGL's Public Shares exercises redemption rights as described in this proxy statement/prospectus and without regard to any shares issuable upon exercise of options or warrants). See the section entitled "*Proposal No. 1—The Business Combination Proposal—Structure of the Transactions.*"
- The Merger Agreement may be terminated at any time, but not later than the closing of the Business Combination, (i) by mutual written consent of LGL and IronNet; (ii) by either LGL or IronNet if the transactions are not consummated on or before the later of November 12, 2021 or such later date as LGL stockholders may approve; (iii) by either LGL or IronNet if a governmental entity shall have issued an order, decree or ruling or taken any other action, in any case having the effect of permanently restraining, enjoining or otherwise prohibiting the Business Combination, which order, decree, judgment, ruling or other action is final and non-appealable; (iv) by either LGL or IronNet if the other party has breached any of its covenants or representations and warranties in any material respect such that the closing conditions regarding the accuracy thereof would not be satisfied, and has not cured its breach within forty-five (45) days (or any shorter time period that remains prior to the termination date provided in item (ii) above) of the notice of an intent to terminate, provided that the terminating party is itself not in breach; (v) by LGL if IronNet stockholder approval of the Business Combination has not been obtained within three business days following the date that this proxy statement/prospectus is disseminated by IronNet to its stockholders; or (vi) by either LGL or IronNet if, at the LGL stockholder meeting, the Business Combination shall fail to be approved by the required vote described herein (subject to any adjournment or recess of the meeting). See the section entitled "*The Merger Agreement—Termination*."
- In addition to voting on the Business Combination proposal, LGL stockholders will vote on separate proposals to approve amendments to LGL's current amended and restated certificate of incorporation

to: (i) change the name of the public entity to "IronNet, Inc." as opposed to "LGL Systems Acquisition Corp."; (ii) increase LGL's capitalization so that it will have 500,000,000 authorized shares of a single class of common stock and 100,000,000 authorized shares of preferred stock, as opposed to LGL having 75,000,000 authorized shares of Class A common stock, 10,000,000 authorized shares of Class B common stock and 1,000,000 authorized shares of preferred stock; (iii) require that stockholders only act at annual and special meeting of the corporation and not by written consent; (iv) eliminate the current limitations in place on the corporate opportunity doctrine; (v) increase the required vote thresholds to 66 2/3% for stockholders to approve amendments to the bylaws and amendments to certain provisions of the certificate of incorporation; and (vi) delete the various provisions applicable only to special purpose acquisition corporations (such as the obligation to dissolve and liquidate if a business combination is not consummated within a certain period of time) that will no longer be relevant following the consummation of the Business Combination. The stockholders of LGL will also consider and vote upon a proposal to approve, for purposes of complying with applicable listing rules of the NYSE, the issuance by LGL of shares of LGL Class A common stock pursuant to the Business Combination and the issuance by LGL of shares of LGL common stock to certain accredited investors, qualified institutional buyers and qualified purchasers in the Private Placement, the proceeds of which will be used to finance the Business Combination and related transactions and the costs and expenses incurred in connection therewith with any balance used for working capital purposes. LGL stockholders will also vote on proposals (w) to elect eleven (11) directors who, upon consummation of the Business Combination, will become the directors of the Combined Company, (x) to approve the 2021 Plan, (y) to approve the ESPP and (z) to approve, if necessary, an adjournment of the special meeting. See the sections entitled "*Proposal No. 2—The LGL Charter Proposals*," "*Proposal No. 3—The NYSE Proposal*," "*Proposal No. 4—The Director Election Proposal*," "*Proposal No. 5—The Incentive Plan Proposal,*" "*Proposal No. 6—The ESPP Proposal"* and "*Proposal No. 7—The Adjournment Proposal*."

- Upon completion of the Business Combination, if management's nominees are elected, the directors of the Combined Company will be Gen. Keith B. Alexander (Ret.) (IronNet's Co-Chief Executive Officer and Chairman), Donald R. Dixon (a current director of IronNet), Mary E. Gallagher (a current director of LGL), Gen. John M. Keane (Ret.) (a current director of IronNet), Robert "Rob" LaPenta Jr. (a current director of LGL), Vadm. John M. McConnell (Ret.) (a current director of IronNet), André Pienaar (a current director of IronNet), Hon. Michael J. Rogers (a current director of IronNet), Theodore E. Schlein (a current director of IronNet) and Vadm. Jan E. Tighe (Ret.) (a current director of IronNet). See the section entitled "*Proposal No. 4—The Director Election Proposal*."
- Upon completion of the Business Combination, the executive officers of the Combined Company will include Gen. Keith B. Alexander (Ret.) (IronNet's Co-Chief Executive Officer and Chairman), William E. Welch (IronNet's Co-Chief Executive Officer), James C. Gerber (IronNet's Chief Financial Officer), Sean Foster (IronNet's Chief Revenue Officer), Russell Cobb (IronNet's Chief Marketing Officer), Donald Closser (IronNet's Chief Product Officer). See "*Management of the Combined Company*."
- Pursuant to the Registration Rights Agreement, certain IronNet stockholders, the Sponsor, the holders of the Founder Shares and certain other LGL stockholders will be granted certain rights to have registered, in certain circumstances, the resale under the Securities Act of their securities of the Combined Company, subject to certain conditions set forth therein.
- In connection with the execution of the Merger Agreement, certain of IronNet's executive officers, directors and securityholders, who collectively hold securities constituting more than 80% of the voting power represented by the outstanding shares of IronNet common stock and IronNet preferred stock, have agreed to execute and deliver a written consent with respect to the outstanding shares of IronNet common stock and preferred stock held by such holders adopting the Merger Agreement and approving the Business Combination; accordingly, IronNet expects to have the required votes to approve the IronNet merger proposal.

FORWARD-LOOKING STATEMENTS

LGL believes it is important to communicate its expectations to its stockholders. However, there may be events in the future that LGL is not able to predict accurately or over which it has no control. Certain statements in this proxy statement/prospectus may constitute "forward-looking statements" for purposes of the federal securities laws. LGL's forward-looking statements include, but are not limited to, statements regarding LGL, LGL's management team's, IronNet's and IronNet's management team's expectations, hopes, beliefs, intentions or strategies regarding the future. In addition, any statements that refer to projections, forecasts or other characterizations of future events or circumstances, including any underlying assumptions, are forward-looking statements. The words "anticipate," "believe," "continue," "could," "estimate," "expect," "intends," "may," "might," "plan," "possible," "potential," "predict," "project," "should," "will," "would" and similar expressions may identify forward-looking statements, but the absence of these words does not mean that a statement is not forward-looking. Forward-looking statements in this proxy statement/prospectus may include, for example, statements about:

- our ability to consummate the Business Combination;
- the anticipated timing of the Business Combination;
- the expected benefits of the Business Combination;
- the Combined Company's financial and business performance following the Business Combination, including financial projections and business metrics;
- changes in the Combined Company's strategy, future operations, financial position, estimated revenue and losses, projected costs, prospects and plans;
- the implementation, market acceptance and success of the Combined Company's business model and growth strategy;
- IronNet's expectations and forecasts with respect to the size and growth of the cybersecurity industry and IronNet's products and services in particular;
- the ability of IronNet's products and services to meet customers' needs;
- IronNet's ability to compete with others in the cybersecurity industry;
- IronNet's ability to retain pricing power with its products;
- IronNet's ability to grow its market share;
- the Combined Company's ability to attract and retain qualified employees and management;
- the Combined Company's ability to adapt to changes in consumer preferences, perception and spending habits and develop and expand its product offerings and gain market acceptance of its products, including in new geographies;
- the Combined Company's ability to develop and maintain IronNet's brand and reputation;
- developments and projections relating to IronNet's competitors and industry;
- the impact of the COVID-19 pandemic on IronNet's business and on the economy in general;
- IronNet's expectations regarding its ability to obtain and maintain intellectual property protection and not infringe on the rights of others;
- expectations regarding the time during which the Combined Company will be an emerging growth company and a smaller reporting company under SEC rules;
- the Combined Company's future capital requirements and sources and uses of cash;
- the Combined Company's ability to obtain funding for its operations and future growth; and
- the Combined Company's business, expansion plans and opportunities.

These forward-looking statements are based on information available as of the date of this proxy statement/prospectus, and current expectations, forecasts and assumptions, and involve a number of judgments, risks and uncertainties. Accordingly, forward-looking statements should not be relied upon as representing our views as of any subsequent date, and we do not undertake any obligation to update forward-looking statements to reflect events or circumstances after the date they were made, whether as a result of new information, future events or otherwise, except as may be required under applicable securities laws.

You should not place undue reliance on these forward-looking statements in deciding how to vote your proxy or instruct how your vote should be cast on the proposals set forth in this proxy statement/prospectus. As a result of a number of known and unknown risks and uncertainties, our actual results or performance may be materially different from those expressed or implied by these forward-looking statements. Some factors that could cause actual results to differ include:

- the occurrence of any event, change or other circumstances that could delay the Business Combination or give rise to the termination of the Merger Agreement;
- the outcome of any legal proceedings that may be instituted against LGL or IronNet following announcement of the proposed Business Combination and transactions contemplated thereby;
- the inability to complete the Business Combination due to the failure to obtain approval of the stockholders of LGL or to satisfy other conditions to the closing of the proposed Merger in the Business Combination Agreement;
- the ability to obtain or maintain the listing of LGL's securities on the NYSE following the Business Combination;
- the risk that the proposed Business Combination disrupts current plans and operations of IronNet as a result of the consummation of the transactions described herein;
- the potential liquidity and trading of LGL's public securities;
- the inability to recognize the anticipated benefits of the proposed Business Combination, which may be affected by, among other things, the amount of cash available following any redemption of public shares by LGL stockholders;
- the ability of the Combined Company to execute its business model and operate in highly competitive markets, and potential adverse effects of this competition;
- risk of decreased revenues due to pricing pressures;
- the Combined Company's ability to attract, motivate and retain qualified employees, including members of its senior management team;
- the Combined Company's ability to maintain a high level of client service and expand operations;
- potential failure to comply with privacy and information security regulations governing the client datasets IronNet processes and stores;
- the risk that IronNet or the Combined Company is unsuccessful in integrating potential acquired businesses and product lines;
- potential issues with IronNet's product offerings that could cause legal exposure, reputational damage and an inability to deliver products or services;
- the ability of the Combined Company to develop new products, improve existing products and adapt its business model to keep pace with industry trends;
- the risk that IronNet's products and services fail to interoperate with third-party systems;
- the ability to maintain effective controls over disclosure and financial reporting that enable the Combined Company to comply with regulations and produce accurate financial statements;

- the potential disruption of IronNet's products, offerings, website and networks;
- the ability to deliver products and services following a disaster or business continuity event;
- increased risks resulting from IronNet's international operations;
- potential unauthorized use of IronNet's products and technology by third parties;
- global economic conditions;
- the impact of health epidemics, including the COVID-19 pandemic, on IronNet's business and the actions IronNet or the Combined Company may take in response thereto;
- exchange rate fluctuations and volatility in global currency markets;
- changes in applicable laws or regulations;
- the ability to comply with various trade restrictions, such as sanctions and export controls;
- potential intellectual property infringement claims;
- the ability to comply with the anti-corruption laws of the United States and various international jurisdictions;
- potential impairment charges related to goodwill, identified intangible assets and fixed assets;
- potential litigation involving LGL or IronNet following the consummation of the Business Combination;
- costs related to the Business Combination;
- the Combined Company's ability to raise capital; and
- other risks and uncertainties indicated in this proxy statement/prospectus, including those set forth under the section entitled "*Risk Factors*."

Before you grant your proxy or instruct your bank or broker how to vote, or vote on the Business Combination proposal, the LGL charter proposals, the NYSE proposal, the director election proposal, the incentive plan proposal, the ESPP proposal or the adjournment proposal, you should be aware that the occurrence of the events described in the section entitled "*Risk Factors*" and elsewhere in this proxy statement/prospectus may adversely affect LGL and/or IronNet.

RISK FACTORS

The Combined Company will face a market environment that cannot be predicted and that involves significant risks, many of which will be beyond its control. In addition to the other information contained in this proxy statement/prospectus, stockholders should carefully consider the following risk factors, together with all of the other information included in this proxy statement/prospectus, before they decide whether to vote or instruct their vote to be cast to approve the proposals described in this proxy statement/prospectus.

The value of your investment in the Combined Company following consummation of the Business Combination will be subject to the significant risks affecting IronNet and inherent to the industry in which it operates. You should carefully consider the risks and uncertainties described below and other information included in this proxy statement/prospectus. If any of the events described below occur, the Combined Company's business and financial results could be adversely affected in a material way. This could cause the trading price of its common stock to decline, perhaps significantly, and you therefore may lose all or part of your investment.

Risks Related to IronNet's Business and Industry

IronNet has experienced rapid growth in recent periods, and if the Combined Company does not manage its future growth, its business and results of operations will be adversely affected.

IronNet has experienced rapid revenue growth in recent periods, and following the Business Combination the Combined Company expects to continue to invest broadly across its organization to support its growth. For example, IronNet's headcount grew from 196 full-time employees as of January 31, 2019 to 246 full-time employees as of January 31, 2021. Although IronNet has experienced rapid growth historically, following the Business Combination, the Combined Company may not be able sustain IronNet's current growth rates, nor can we assure you that the Combined Company's investments to support its growth will be successful. The growth and expansion of the Combined Company's business will require it to invest significant financial and operational resources and the continuous dedication of its management team. IronNet has encountered, and the Combined Company will continue to encounter, risks and difficulties frequently experienced by rapidly growing companies in evolving industries, including market acceptance of its products, adding new customers, intense competition, and its ability to manage its costs and operating expenses. The Combined Company's future success will depend in part on its ability to manage its growth effectively, which will require the Combined Company to, among other things:

- effectively attract, integrate and retain a large number of new employees, particularly members of its sales and marketing, data science, and research and development teams;
- further improve its platform and products, including its cloud modules and security capabilities, analytics, collective defense capabilities, and visualizations, and IT infrastructure, including expanding and optimizing its data centers, collection, and analytic capabilities, to support its business needs;
- enhance its information and communication systems to ensure that its employees and offices around the world are well coordinated and can effectively communicate with each other and its growing base of customers and partners; and
- improve its financial, management, and compliance systems and controls.

If the Combined Company fails to achieve these objectives effectively, its ability to manage its expected growth, ensure uninterrupted operation of its platform and key business systems, and comply with the rules and regulations applicable to its business could be impaired. Additionally, the quality of its platform and services could suffer and it may not be able to adequately address competitive challenges. Any of the foregoing could adversely affect the Combined Company's business, results of operations, and financial condition.

IronNet has a history of losses and the Combined Company may not be able to achieve or sustain profitability in the future.

IronNet has incurred net losses in all periods since its inception. IronNet experienced net losses of $55.4 million and $47.9 million for fiscal 2021 and fiscal 2020, respectively. As of January 31, 2021, IronNet had an accumulated deficit of $175.0 million. While IronNet has experienced significant growth in revenue in recent periods, we cannot predict when or whether the Combined Company will reach or maintain profitability. We also expect the Combined Company's operating expenses to increase over IronNet's historical expenses in the future as the Combined Company continues to invest for future growth, which will negatively affect its results of operations if its total revenue does not increase. We cannot assure you that these investments will result in substantial increases in its total revenue or improvements in its results of operations. In addition to the anticipated costs to grow the Combined Company's business, we also expect to incur significant additional legal, accounting, and other expenses as a newly public operating company. Any failure to increase the Combined Company's revenue as it invests in its business or to manage its costs could prevent it from achieving or maintaining profitability or positive cash flow.

IronNet's limited operating history makes it difficult to evaluate its current business and the Combined Company's future prospects and may increase the risk of your investment.

IronNet was founded in 2014 and launched its first cybersecurity network detection and response product in 2016 (IronDefense) and its first collective defense product in 2018 (IronDome). IronNet's limited operating history makes it difficult to evaluate its current business, the Combined Company's future prospects, and other trends, including its ability to plan for and model future growth. IronNet has encountered, and the Combined Company will continue to encounter, risks, uncertainties, and difficulties frequently experienced by rapidly growing companies in evolving industries, including its ability to achieve broad market acceptance of cloud-enabled, and/or software as a service ("*SaaS*") delivered cybersecurity solutions and its platform, attract additional customers, grow partnerships, compete effectively, build and maintain effective compliance programs, and manage increasing expenses as it continues to invest in its business. If the Combined Company does not address these risks, uncertainties and difficulties successfully, its business, and results of operations will be harmed. Further, IronNet has limited historical financial data and operates in a rapidly evolving market. As a result, any predictions about the Combined Company's future revenue and expenses may not be as accurate as they would be if IronNet had a longer operating history or operated in a more predictable market.

The COVID-19 pandemic could adversely affect the Combined Company's business, operating results and future revenue.

In March 2020, the World Health Organization declared COVID-19 a global pandemic. This contagious disease outbreak has spread across the globe and is impacting worldwide economic activity and financial markets. In light of the uncertain and rapidly evolving situation relating to the spread of COVID-19, IronNet has taken precautionary measures intended to mitigate the spread of the virus and minimize the risk to its employees, customers, partners, and the communities in which it operates. These measures include transitioning its employee population to work remotely from home, imposing travel restrictions for its employees, shifting customer, partner and investor events to virtual-only formats, and limiting capacity at any of its offices which have reopened or may reopen during the pandemic's duration. These precautionary measures, many of which IronNet has now made largely permanent and sustainable, and associated economic issues, both in the United States and across the globe, could negatively affect IronNet's CS efforts, significantly delay and lengthen its sales cycles, impact its sales and marketing efforts, reduce employee efficiency and productivity, slow its international expansion efforts, increase cybersecurity risks, and create operational or other challenges, any of which could harm its business and results of operations. Moreover, due to IronNet's subscription-based business model, the effect of the COVID-19 pandemic may not be fully reflected in the Combined Company's results of operations until future periods, if at all.

In addition, the COVID-19 pandemic may disrupt the operations of IronNet's prospective clients, customers, and partners for an indefinite period of time. Some of its customers have been negatively impacted by the COVID-19 pandemic, which could result in delays in accounts receivable collection, or result in decreased technology spending, including spending on cybersecurity, which could negatively affect the Combined Company's revenues. Some of its prospective clients have also been negatively impacted by the COVID-19 pandemic, which could result in delays in sales or lengthen purchasing decisions.

More generally, the COVID-19 pandemic has adversely affected economies and financial markets globally, and continued uncertainty could lead to a prolonged economic downturn, which could result in a larger customer turnover than is currently anticipated, reduced demand for IronNet's products and services, and increased length of sales cycles, in which case the Combined Company's revenues could be significantly impacted. The impact of the COVID-19 pandemic may also exacerbate other risks discussed in this "Risk Factors" section and elsewhere in this proxy statement/prospectus. It is not possible at this time to estimate the impact that the COVID-19 pandemic could have on the Combined Company's business, as the impact will depend on future developments, which are highly uncertain and cannot be predicted.

If organizations do not adopt cloud-enabled, and/or SaaS-delivered cybersecurity solutions that may be based on new and untested security concepts, the Combined Company's ability to grow its business and results of operations may be adversely affected.

The Combined Company's future success depends on the growth in the market for cloud-enabled and/or SaaS-delivered cybersecurity solutions. The use of SaaS solutions to manage and automate security and IT operations is rapidly evolving. As such, it is difficult to predict its potential growth, customer adoption and retention rates, customer demand for IronNet's solutions, or the success of existing or future competitive products. Any expansion in IronNet's market depends on a number of factors, including the cost, performance and perceived value associated with its solutions and those of its competitors. If IronNet's solutions do not achieve widespread adoption or there is a reduction in demand for its solutions due to a lack of customer acceptance, technological challenges, competing products, privacy or other liability concerns, decreases in corporate spending, weakening economic conditions, or otherwise, it could adversely affect the Combined Company's business, results of operations and financial results, resulting from such things as early terminations, reduced customer retention rates, or decreased sales. We do not know whether the trend in adoption of cloud-enabled and/or SaaS-delivered cybersecurity solutions that IronNet has experienced in the past will continue in the future. Furthermore, if IronNet or other SaaS security providers experience security incidents, loss, or disclosure of customer data, disruptions in delivery, or other problems, the market for SaaS solutions as a whole, including IronNet's security solutions, could be negatively affected.

In addition to reliance on a cloud-enabled and/or SaaS-delivered model, the cybersecurity solutions of the Combined Company utilize a novel and relatively new approach to collective defense that relies on customers sharing sensitive customer information with the Combined Company. Some of that raw customer information may contain personal or confidential information, or data perceived to be personal or confidential information. From that customer information, the Combined Company generates analytics that allow it to deliver threat knowledge and network intelligence at machine speed across a wide variety of industries. Because this new approach requires the sharing of sensitive customer information, concerns may exist that sharing of the customer information may violate, or be perceived as potentially violating, privacy laws or providing a competitive advantage to another entity. As a result, some current or prospective customers may decide not to procure the Combined Company's products or share any customer information. Such lack of acceptance could have negative effects on the Combined Company, including reduced or lost revenues or inadequate information being available for the Combined Company's analysis, thus making its products less effective. In addition, uncertainties about the regulatory environment concerning personal information and the potential liability raised by sharing such information could further inhibit the broad-scale adoption of its solutions.

Historically, information sharing related to cybersecurity has been a very well accepted concept from a theoretical perspective but very difficult to implement in practice. Companies are generally reluctant to share their sensitive cyber information with other entities, despite knowing the advantages of doing so. Although raw customer information will not be shared with other parties, it does undergo filtering, concatenation, and other transformations within the IronNet solutions with the goal of removing any sensitive or personal information. Misperceptions may exist, however, about what information gets shared, with whom that information is shared, and the jurisdictions (including foreign countries) of the companies with which the information gets shared. Further, concerns of existing or potential customers may exist related to the ability to completely remove any indicia of the source company, general market rejection of information sharing, or specific market skepticism of IronNet's approach to collective defense, which may further add to a lack of customer acceptance.

In addition to the potential concerns related to sharing sensitive information in a system consisting of commercial or potentially competitive entities, additional concerns can arise when governments become involved as participants in the collective defense ecosystem. From a commercial perspective, companies frequently view information sharing with governments as risky, based on perceptions that the governments might use such shared information to take action against the companies or to otherwise utilize it in a way that will expose such companies to liability. Such perceptions could lead commercial entities to stop sharing, not procure IronNet's services in the first place, or terminate their relationship with the Combined Company altogether. Similarly, governments (as customers) may be unable to properly process such data or utilize it in a meaningful way, or share useful information back into the IronNet solutions. Any of these concerns could lead to reduced sales or contribute to a lack of customer acceptance. In addition, the mere involvement of one or more government entities may harm the Combined Company's reputation with certain companies.

If the Combined Company is unable to attract new customers, its future results of operations could be harmed.

To expand its customer base, the Combined Company will need to convince potential customers to allocate a portion of their discretionary budgets to purchase IronNet's platform and solutions. IronNet's sales efforts have often involved educating its prospective customers about the uses and benefits of its platform and solutions. Enterprises and governments that use legacy security products, such as signature-based or malware-focused products, firewalls, intrusion prevention systems and endpoint technologies, may be hesitant to purchase IronNet's platform and solutions if they believe that legacy security products are more cost effective, provide substantially the same functionality as IronNet's platform and solutions or provide a level of cybersecurity that is sufficient to meet their needs.

The Combined Company may have difficulty convincing prospective customers of the value of adopting IronNet's solutions. Even if the Combined Company is successful in convincing prospective customers that a cloud-enabled platform like IronNet's is critical to protect against cyberattacks, they may not decide to purchase IronNet's platform and solutions for a variety of reasons, some of which are out of IronNet's control. For example, any future deterioration in general economic conditions, including a downturn due to the outbreak of diseases such as COVID-19, may cause IronNet's current and prospective customers to cut their overall security and IT operations spending, and such cuts may fall disproportionately on cloud-based security solutions. Economic weakness, customer financial difficulties, and constrained spending on security and IT operations may result in decreased revenue and adversely affect the Combined Company's results of operations and financial condition. Additionally, if the incidence of cyberattacks were to decline, or enterprises or governments perceive that the general level or relative risk of cyberattacks has declined, the Combined Company's ability to attract new customers and expand sales of IronNet's solutions to existing customers could be adversely affected. If organizations do not continue to adopt IronNet's platform and solutions, the Combined Company's sales will not grow as quickly as anticipated, or at all, and its business, results of operations, and financial condition would be harmed.

If IronNet's customers do not renew their subscriptions for its products, the Combined Company's future results of operations could be harmed.

In order for the Combined Company to maintain or improve its results of operations, it is important that IronNet's customers renew their subscriptions for its platform and solutions when existing contract terms expire, and that the Combined Company expands its commercial relationships with IronNet's existing customers by selling additional subscriptions. IronNet's customers have no obligation to renew their subscriptions after the expiration of their contractual subscription period, which is generally one year, and in the normal course of business, some customers have elected not to renew. In addition, IronNet's customers may renew for shorter contract subscription lengths or cease using certain solutions. IronNet's customer retention and expansion may decline or fluctuate as a result of a number of factors, including its customers' satisfaction with its services, its pricing, customer security and networking issues and requirements, its customers' spending levels, mergers and acquisitions involving its customers, industry developments, competition and general economic conditions. If the Combined Company's efforts to maintain and expand its relationships with IronNet's existing customers are not successful, the Combined Company's business, results of operations, and financial condition may materially suffer.

As a first mover in collective defense for the commercial sector, IronNet may face significant liability if it is unable to effectively anonymize and safeguard its clients' data.

IronNet is the first major commercial vendor to offer an end-to-end means to take full advantage of the collective defense concept that relies on customers sharing sensitive customer information with IronNet. While raw customer information is not shared with other parties and shared data undergoes filtering and other transformations within the IronNet solution, with the goal of removing any sensitive or personal information, it is possible that customer information could be accessed by third parties (including competitors of IronNet's clients), through a failure of IronNet's procedures to effectively anonymize the shared data or as a result of hackers gaining access to the raw data collected by IronNet. To the extent IronNet is not able to effectively anonymize and protect its customers' data, it may be subject to liability, which could adversely affect its business, results of operations and financial condition. In addition, given the novelty of IronNet's approach, it is possible that other risks could surface of which IronNet is currently unaware.

Competition from existing or new companies could cause IronNet to experience downward pressure on prices, fewer customer orders, reduced margins, the inability to take advantage of new business opportunities and loss of market share.

The market for cybersecurity solutions is intensely competitive, fragmented, and characterized by rapid changes in technology, customer requirements, industry standards, increasingly sophisticated attackers, and by frequent introductions of new or improved products to combat security threats. We expect the Combined Company to continue to face intense competition from IronNet's current competitors, as well as from new entrants into the market. If the Combined Company is unable to anticipate or react to these challenges, its competitive position could weaken, and it could experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect its business, financial condition and results of operations. The ability to compete effectively will depend upon numerous factors, many of which are beyond IronNet's control, including, but not limited to:

- product capabilities, including performance and reliability, of its platform, including its services and features particularly in the areas of analytics and collective defense, compared to those of its competitors;
- its ability, and the ability of its competitors, to improve existing products, services and features, or to develop new ones to address evolving customer needs;
- its ability to attract, retain and motivate talented employees;

- its ability to establish, capitalize on, maintain, and grow relationships with distribution and technology partners;
- the strength of its sales and marketing efforts; and
- acquisitions or consolidation within its industry, which may result in more formidable competitors.

IronNet's competitors include the following companies by general category:

- First generation Network Detection and Response (NDR) vendors such as DarkTrace or Vectra Networks, who offer point products based on Bayesian analysis, outlier analysis, and heuristic detection-based detection;
- Network security vendors, such as Cisco and Palo Alto Networks, Inc., who are supplementing their core network security additional behavioral-based detection with behavioral-based detection, threat intelligence and security operations solutions; and
- Legacy network infrastructure and performance monitoring companies such as ExtraHop and Arista Networks, who are adding security use cases to their infrastructure products.

Many of these competitors have greater financial, technical, marketing, sales, and other resources, greater name recognition, longer operating histories, and a significantly larger base of customers than IronNet does. They may be able to devote greater resources to the development, promotion, and sale of services than the Combined Company can, and they may offer lower pricing than IronNet does. Further, they may have greater resources for research and development of new technologies, the provision of customer support, and the pursuit of acquisitions, or they may have other financial, technical or other resource advantages. IronNet's larger competitors have substantially broader and more diverse product and services offerings as well as routes to market, which may allow them to leverage their relationships based on other products, or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing IronNet's products.

Conditions in IronNet's market could change rapidly and significantly as a result of technological advancements, partnering or acquisitions by competitors or continuing market consolidation. Some of IronNet's current or potential competitors have made or could make acquisitions of businesses or establish cooperative relationships that may allow them to offer more directly competitive and comprehensive solutions than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in the market or the Combined Company's failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, increased net losses and loss of market share. Further, many competitors that specialize in providing protection from particular types of security threats may be able to deliver these more targeted security products to the market quicker than the Combined Company can or may be able to convince organizations that these more limited products meet their needs.

Even if there is significant demand for cloud-based security solutions like IronNet's or if its competitors include functionality that is, or is perceived to be, equivalent to or better than IronNet's in legacy products that are already generally accepted as necessary components of an organization's cybersecurity architecture, the Combined Company may have difficulty increasing the market penetration of IronNet's platform. Furthermore, even if the functionality offered by other security and IT operations providers is different and more limited than the functionality of IronNet's platform, organizations may elect to accept such limited functionality in lieu of adding products from additional vendors like IronNet. If the Combined Company is unable to compete successfully, its business, financial condition, and results of operations would be adversely affected.

Competitive pricing pressure may reduce gross profits and adversely affect the Combined Company's financial results.

If the Combined Company is unable to maintain IronNet's pricing due to competitive pressures or other factors, its margins may be reduced and its gross profits, business, results of operations and financial condition

may be adversely affected. The subscription prices for IronNet's platform, solutions, and professional services may decline for a variety of reasons, including competitive pricing pressures, discounts, anticipation of the introduction of new solutions by competitors, or promotional programs offered by the Combined Company or its competitors. Competition continues to increase in the market segments in which IronNet operates, and we expect competition to further increase in the future. Larger competitors with more diverse product and service offerings may reduce the price of products or subscriptions that compete with IronNet's or may bundle them with other products and subscriptions in an effort to leverage their existing market share to make it harder for newer companies, like IronNet, to effectively compete.

If IronNet's solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, its brand and reputation would be harmed, which would adversely affect the Combined Company's business and results of operations.

Real or perceived defects, errors, or vulnerabilities in IronNet's platform and solutions, the failure of its platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of its solutions, actions or inactions by employees or contractors that create vulnerabilities in its platform or solutions, or the failure of customers to take action on attacks identified by its platform could harm IronNet's reputation and adversely affect the Combined Company's business, financial position, and results of operations. Because its cloud-enabled security platform is complex, it may contain defects or errors that are not detected until after deployment. We cannot assure you that IronNet's products will detect all cyberattacks, especially in light of the rapidly changing security threat landscape that its solution seeks to address. Due to a variety of both internal and external factors, including, without limitation, defects or misconfigurations of its solutions, its solutions could become vulnerable to security incidents (both from intentional attacks and accidental causes) that cause them to fail to secure networks and detect and block attacks. In addition, because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that IronNet's cloud-enabled security platform is unable to detect or prevent until after some of its customers are affected. For example, certain computer hackers may be supported or directly employed by so-called nation-states, which are generally defined as sovereign territories with individuals who share a common history and set of ideals. In the context of cybersecurity, certain aggressive nation-states with a history of disregarding generally acceptable computer network norms may employ particularly sophisticated and experienced actors who focus on being persistent, unpredictable, and innovative, with the ability to tap into significant nation-state budgets. This allows such nation-state attackers to develop expansive attack playbooks and access to cutting-edge technology to facilitate their attacks, including new, or so-called zero-day, attacks. Such nation-state attackers could successfully attack IronNet or an IronNet customer, which could significantly harm the Combined Company's reputation. Additionally, IronNet's platform may falsely indicate a cyberattack or threat that does not actually exist, which may lessen customers' trust in its solutions.

Moreover, as its cloud-enabled security platform is adopted by an increasing number of enterprises and governments, it is possible that the individuals and organizations behind advanced cyberattacks will begin to focus on finding ways to defeat its security platform. If this happens, IronNet's systems and subscription customers could be specifically targeted by attackers and could result in vulnerabilities in its platform or undermine the market acceptance of its platform and could adversely affect its reputation as a provider of security solutions. Because IronNet hosts customer data on its cloud and other platforms, which in some cases may contain personally identifiable information ("*PII*") or potentially confidential information, a security compromise, or an accidental or intentional misconfiguration or malfunction of its platform could result in PII and other customer data being accessible to attackers or to other customers. Further, if a high-profile security breach occurs with respect to another next-generation or cloud-enabled security system, IronNet's customers and potential customers may lose trust in such solutions generally, and cloud-enabled security solutions in particular.

Organizations are increasingly subject to a wide variety of attacks on their networks, systems, and endpoints. No security solution, including IronNet's platform, can address all possible security threats or block

If IronNet does not effectively expand and train its direct sales force, it may be unable to add new customers or increase sales to existing customers, and its business will be adversely affected.

IronNet depends on its direct sales force to obtain new customers and increase sales with existing customers. Its ability to achieve significant revenue growth will depend, in large part, on its success in recruiting, training and retaining sufficient numbers of sales personnel, particularly in international markets. IronNet has expanded its sales organization significantly in recent periods and expect to continue to add additional sales capabilities in the near term. There is significant competition for sales personnel with the skills and technical knowledge that IronNet requires. New hires require significant training and may take significant time before they achieve full productivity, and this delay is accentuated by IronNet's long sales cycles. IronNet's recent hires and planned hires may not become productive as quickly as it expects, and the Combined Company may be unable to hire or retain sufficient numbers of qualified individuals in the markets where IronNet does business or plans to do business. In addition, a large percentage of IronNet's salesforce is new to its business and selling its solutions, and therefore this team may be less effective than its more seasoned sales personnel. Furthermore, hiring sales personnel in new countries, or expanding its existing presence, requires upfront and ongoing expenditures that IronNet may not recover if the sales personnel fail to achieve full productivity. We cannot predict whether, or to what extent, the Combined Company's sales will increase as it expands its sales force or how long it will take for sales personnel to become productive. If the Combined Company is unable to hire and train a sufficient number of effective sales personnel, or the sales personnel it hires are not successful in obtaining new customers or increasing sales to IronNet's existing customer base, the Combined Company's business and results of operations will be adversely affected.

Because IronNet recognizes revenue from subscriptions to its platform and other forms of providing customers with access to its software over the term of the subscription or contract, downturns or upturns in new business will not be immediately reflected in the Combined Company's results of operations.

IronNet generally recognizes revenue from customers ratably over the terms of their subscription or contract term, which average over three years in length, though may be as short as one year or less. As a result, a substantial portion of the revenue that IronNet reports in each period is attributable to the recognition of deferred revenue relating to agreements that it entered into during previous periods. Consequently, any increase or decline in new sales or renewals in any one period will not be immediately reflected in its revenue for that period. Any such change, however, would affect its revenue in future periods. Accordingly, the effect of downturns or upturns in new sales and potential changes in IronNet's rate of renewals may not be fully reflected in the Combined Company's results of operations until future periods.

A limited number of customers represent a substantial portion of IronNet's revenue. If the Combined Company fails to retain these customers, its revenue could decline significantly.

IronNet derives a substantial portion of its revenue from a limited number of customers. For fiscal 2021 and fiscal 2020, six customers accounted for 46% and four customers accounted for 48% of IronNet's revenues, respectively. As of January 31, 2021 and 2020, three customers represented 85% and one customer represented 30%, respectively, of IronNet's total accounts receivable balance. As a result, the Combined Company's revenue could fluctuate materially and could be materially and disproportionately impacted by purchasing decisions of these customers or any other significant future customer. Any of the Combined Company's significant customers may decide to purchase less than they have in the past, may alter their purchasing patterns at any time with limited notice, or may decide not to continue to license IronNet's products at all, any of which could cause the Combined Company's revenue to decline and adversely affect its financial condition and results of operations. If the Combined Company does not further diversify IronNet's customer base, it will continue to be susceptible to risks associated with customer concentration.

IronNet's results of operations may fluctuate significantly, which could make its future results difficult to predict and could cause its results of operations to fall below expectations.

IronNet's results of operations have varied significantly from period to period, and we expect that the Combined Company's results of operations will continue to vary as a result of a number of factors, many of which are outside of IronNet's control and may be difficult to predict, including:

- the impact of the COVID-19 pandemic on its operations, financial results, and liquidity and capital resources, including on customers, sales, expenses, and employees;

- its ability to attract new and retain existing customers;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of customers;
- the timing and length of its sales cycles;
- changes in customer or distribution partner requirements or market needs;
- changes in the growth rate of its market;
- the timing and success of new product and service introductions by it or its competitors or any other competitive developments, including consolidation among its customers or competitors;
- the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of its platform;
- its ability to successfully expand its business domestically and internationally;
- decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in its pricing policies or those of its competitors;
- any disruption in its relationship with distribution partners;
- insolvency or credit difficulties confronting its customers, affecting their ability to purchase or pay for its solutions;
- significant security breaches of, technical difficulties with or interruptions to, the use of its platform;
- extraordinary expenses such as litigation or other dispute-related settlement payments or outcomes;
- general economic conditions, both in domestic and foreign markets;
- future accounting pronouncements or changes in its accounting policies or practices;
- negative media coverage or publicity;
- political events;
- the amount and timing of operating costs and capital expenditures related to the expansion of its business; and
- increases or decreases in expenses caused by fluctuations in foreign currency exchange rates.

In addition, IronNet experiences seasonal fluctuations in its financial results as it can receive a higher percentage of its annual orders from new customers, as well as renewal orders from existing customers, in the fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of its customers. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in the Combined Company's financial and other results from period to period. As a result of this variability, IronNet's historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in the Combined Company's failure to meet its operating plan or the expectations of investors or analysts for any period. If it fails to meet such expectations for these or other reasons, the Combined Company' stock price could fall substantially, and it could face costly lawsuits, including securities class action suits.

IronNet's sales cycles can be long and unpredictable, and its sales efforts require considerable time and expense.

IronNet's revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for its platform, particularly with respect to large organizations and government entities. Customers often

view the subscription to its platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test, and qualify its platform and solutions prior to entering into or expanding a relationship with it. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens its sales cycle.

IronNet's direct sales team develops relationships with its customers, and works with its distribution partners on account penetration, account coordination, sales and overall market development. IronNet spends substantial time and resources on its sales efforts without any assurance that its efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals, and unanticipated administrative, processing, and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of IronNet's efforts to secure sales after investing resources in a lengthy sales process could adversely affect its business and results of operations.

IronNet relies heavily on the services of its senior management team and other highly skilled personnel, and if the Combined Company is not successful in attracting or retaining highly qualified personnel, it may not be able to successfully implement IronNet's business strategy.

The Combined Company's future success will be substantially dependent on its ability to attract, retain, and motivate the members of its management team and other key employees throughout its organization. In particular, the Combined Company will be highly dependent on the services of Gen. Keith B. Alexander (Ret.) and William Welch, the co-chief executive officers of the Combined Company, who will be critical to its future vision and strategic direction. It will also rely on its leadership team in the areas of operations, security, analytics, engineering, product management, research and development, marketing, sales, partnerships, mergers and acquisitions, support, and general and administrative functions. Gen. Keith B. Alexander (Ret.) provides IronNet's future growth to key decisionmakers with government and the private sector and his leadership role at the Combined Company will be difficult to replace. Although we expect that the Combined Company will enter into employment agreements with its key personnel following the consummation of the Business Combination, its employees, including its executive officers, will be employed on an "at-will" basis, which means they may terminate their employment with the Combined Company at any time. If one or more of the Combined Company's key employees or members of its management team resigns or otherwise ceases to provide it with their service, its business could be harmed.

If the Combined Company is unable to attract and retain qualified personnel, its business could be harmed.

There is significant competition for personnel with the skills and technical knowledge that the Combined Company will require across its technology, cyber, sales, professional services and administrative support functions. Competition for these personnel in the Washington, D.C. metro area, where the corporate headquarters of the Combined Company will be located, and in other locations where it maintains offices or otherwise operates, is competitive, especially for experienced sales professionals, engineers and data scientists experienced in designing and developing cybersecurity software. Although IronNet's current remote work environment facilitates its ability to attract talent across a wider geographic base, IronNet has from time to time experienced, and we expect the Combined Company to continue to experience, difficulty in hiring and retaining employees with appropriate qualifications. Many of the companies with which IronNet competes for experienced personnel have greater resources than it has. Its competitors also may be successful in recruiting and hiring members of its management team or other key employees, and it may be difficult for the Combined Company to find suitable replacements on a timely basis, on competitive terms, or at all. The Combined Company may also be subject to allegations that employees it hires have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product, or that they have been hired in violation of non-compete provisions or non-solicitation provisions.

In addition, job candidates and existing employees often consider the value of the equity awards they receive in connection with their employment. Volatility or lack of performance in the Combined Company's

stock price may also affect its ability to attract and retain key employees. Following the Business Combination, some of IronNet's employees will become vested in a substantial amount of equity awards, which may give them a material amount of personal wealth. This may make it more difficult for the Combined Company to retain and motivate these employees, and this wealth could affect their decision about whether or not they continue to work for the Combined Company. Any failure to successfully attract, integrate or retain qualified personnel to fulfill its current or future needs could adversely affect its business, results of operations and financial condition.

If the Combined Company is not able to maintain and enhance the IronNet brand and its reputation as a provider of high-efficacy cybersecurity solutions, its business and results of operations may be adversely affected.

We believe that maintaining and enhancing IronNet's brand and its reputation as a provider of high-efficacy cybersecurity solutions is critical to its relationship with its existing customers and distribution partners and its ability to attract new customers and partners. The successful promotion of the IronNet brand will depend on a number of factors, including the Combined Company's investment in marketing efforts, its ability to continue to develop additional features for the IronNet platform, its ability to successfully differentiate its platform from competitive cloud-enabled or legacy security solutions and, ultimately, its ability to detect and remediate cyberattacks. Although we believe it is important for the Combined Company's growth, these brand promotion activities may not be successful or yield increased revenue.

In addition, independent industry or financial analysts and research firms often test IronNet's solutions and provide reviews of its platform, along with the products of its competitors, and perception of its platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of its competitors' products, the IronNet brand may be adversely affected. Its solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of its solutions in real world environments. To the extent potential customers, industry analysts, or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that its solutions or services do not provide significant value, the Combined Company may lose customers, and its reputation, financial condition, and business would be harmed. Additionally, the performance of its distribution partners may affect its brand and reputation if customers do not have a positive experience with these partners. In addition, IronNet has in the past worked, and the Combined Company will continue to work, with high profile customers as well as assist in analyzing and remediating high profile cyberattacks. This work with such customers and cyberattacks may expose the Combined Company to negative publicity and media coverage. Negative publicity, including about the efficacy and reliability of IronNet's platform, its products offerings, its professional services and the customers it works with, even if inaccurate, could adversely affect the Combined Company's reputation and brand.

If the Combined Company is unable to maintain successful relationships with IronNet's distribution partners, or if its distribution partners fail to perform, the Combined Company's ability to market, sell and distribute IronNet's platform and solutions efficiently will be limited, and its business, financial position and results of operations will be harmed.

In addition to its direct sales force, IronNet relies on certain key distribution partners to sell and support its platform. An increasing amount of IronNet's sales flow through its distribution partners, and IronNet expects its reliance on such partners to continue to grow for the foreseeable future. Additionally, IronNet has entered into, and the Combined Company intends to continue to enter into, partnerships with third parties to support its future growth plans. The loss of a substantial number of distribution partners, or the failure to recruit additional partners, could adversely affect the Combined Company's results of operations. The Combined Company's ability to achieve revenue growth in the future will depend in part on its success in maintaining successful relationships with IronNet's distribution partners and in training them to independently sell and deploy IronNet's platform. If the Combined Company fails to effectively manage IronNet's existing sales channels, or if IronNet's distribution partners are unsuccessful in fulfilling the orders for its solutions, or if the Combined Company is

unable to recruit and retain a sufficient number of high quality distribution partners who are motivated to sell IronNet's products, the Combined Company's ability to sell its products and results of operations will be harmed.

IronNet's business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could have an adverse effect on the Combined Company's business and results of operations.

IronNet's future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable, subject to budgetary uncertainty and typically involves long sales cycles. IronNet has made significant investments to address the government sector, but we cannot assure you that these investments will be successful, or that the Combined Company will be able to maintain or grow its revenue from the government sector. Although we anticipate that they may increase in the future, sales to U.S. federal, state and local governmental agencies have not accounted for, and may never account for, a significant portion of the Combined Company's revenue. U.S. federal, state and local government sales are subject to a number of challenges and risks that may adversely impact the Combined Company's business. Sales to such government entities include the following risks:

- selling to governmental agencies can be highly competitive, expensive and time-consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;
- government certification requirements applicable to IronNet's products may change and, in doing so, restrict the Combined Company's ability to sell into the U.S. federal government sector until it has attained the required certifications.
- government demand and payment for IronNet's platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for its platform;
- governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying IronNet's platform, which would adversely impact the Combined Company's revenue and results of operations, or institute fines or civil or criminal liability if the audit were to uncover improper or illegal activities;
- interactions with the U.S. federal government may be limited by post-employment ethics restrictions on members of IronNet's management;
- foreign governments may have concerns with purchasing security products from a company that employs former NSA employees and officials, which may negatively impact sales; and
- governments may require certain products to be manufactured, hosted, or accessed solely in their country or in other relatively high-cost manufacturing locations, and the Combined Company may not manufacture all products in locations that meet these requirements, affecting its ability to sell these products to governmental agencies.

IronNet has achieved Federal Risk and Authorization Management Program ("*FedRAMP*") "FedRAMP-ready" status, but such status is only available for a certain period of time before which it must be utilized. If not utilized, IronNet would likely have to go through certain parts of the FedRAMP process again in order to sell its products to government agencies. Moreover, even if IronNet were to achieve FedRAMP-certified status, such certification is costly to maintain, and if the Combined Company were to lose such a certification in the future it would restrict its ability to sell to government customers. It is also possible that additional guidelines and/or certifications, such as the Cybersecurity Maturity Model Certification ("*CMMC*"), will be required to expand participation in the government sectors.

The occurrence of any of the foregoing could cause governments and governmental agencies to delay or refrain from purchasing IronNet's solutions in the future or otherwise have an adverse effect on the Combined Company's business and results of operations.

The Combined Company may not scale and adapt IronNet's existing technology in a timely and cost-effective manner to meet its customers' performance and other requirements.

The Combined Company's future growth will be dependent upon its ability to continue to meet the needs of new customers and the expanding needs of IronNet's existing customers as their use of its solutions grows. As IronNet's customers gain more experience with its solutions, the number of events, the amount of data transferred, processed, and stored by it, the number of locations where its platform and services are being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of IronNet's customers, the Combined Company intends to continue to make significant investments to increase capacity and to develop and implement new technologies in its service and cloud infrastructure operations. These technologies, which include databases, applications, and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new, and untested. The Combined Company may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop, and test improvements to IronNet's technologies and infrastructure, and the Combined Company may not be able to accurately forecast demand or predict the results it will realize from such improvements. To the extent that the Combined Company does not effectively scale IronNet's operations to meet the needs of its growing customer base and to maintain performance as its customers expand their use of its solutions, the Combined Company may not be able to grow as quickly as anticipated, customers may reduce or cancel use of IronNet's solutions and the Combined Company may be unable to compete as effectively and its business and results of operations may be harmed.

Additionally, IronNet has made, and the Combined Company will continue to make, substantial investments to support growth at its data centers partners and improve the profitability of its cloud platform. If the Combined Company's cloud-based server costs were to increase or pricing pressure causes price movements out of proportion with changes in unit operating costs, its business, results of operations and financial condition may be adversely affected. Although we expect that the Combined Company could receive similar services from other third parties, if any of IronNet's arrangements with third-party providers are terminated, IronNet could experience interruptions on its platform and in its ability to make its solutions available to customers, as well as delays and additional expenses in arranging alternative cloud infrastructure services. Ongoing improvements to cloud infrastructure may be more expensive than anticipated and may not yield the expected savings in operating costs or the expected performance benefits. In addition, the Combined Company may be required to re-invest any cost savings achieved from IronNet's prior cloud infrastructure improvements in future infrastructure projects to maintain the levels of service required by its customers. The Combined Company may not be able to maintain or achieve cost savings from its investments, which could harm its financial results.

The market opportunity estimates and growth forecasts included in this proxy statement/prospectus could prove to be inaccurate, and any real or perceived inaccuracies may harm the Combined Company's reputation and negatively affect its business.

This proxy statement/prospectus includes IronNet's estimates of the addressable market for its cloud-based SaaS-delivered cybersecurity solution. Market opportunity estimates and growth forecasts, whether obtained from third-party sources or developed internally, are subject to significant uncertainty and are based on assumptions and estimates that may not prove to be accurate. The estimates and forecasts in this proxy statement/prospectus relating to the size and expected growth of IronNet's target markets may prove to be inaccurate. In particular, the estimates regarding IronNet's current and projected market opportunity are difficult to predict. In addition, its estimates of the addressable market for cloud-based SaaS-delivered cybersecurity solutions reflect the opportunity available from all participants and potential participants in the market, and IronNet cannot predict with precision its ability to address this demand or the extent of market adoption of its solutions. The addressable

market IronNet estimates may not materialize for many years, if ever, and even if the markets in which it competes meet the size estimates and growth forecasted in this proxy statement/prospectus, the Combined Company's business could fail to grow at similar rates, if at all. Accordingly, the forecasts of market growth included in this proxy statement/prospectus should not be taken as indicative of its future growth.

The success of the Combined Company's business will depend in part on its ability to protect and enforce its intellectual property rights.

We believe that IronNet's intellectual property will be an essential asset of the Combined Company's business, and its success and ability to compete will depend in part upon protection of intellectual property rights. IronNet has relied, and the Combined Company will continue to rely, on a combination of patent, copyright, trademark, and trade secret laws, as well as confidentiality procedures and contractual provisions, to establish and protect its intellectual property rights in the United States and abroad, all of which provide only limited protection. The efforts IronNet has taken to protect its intellectual property may not be sufficient or effective, and its trademarks, copyrights and patents may be held invalid or unenforceable. Moreover, we cannot assure you that any patents will be issued with respect to IronNet's currently pending patent applications, including in a manner that will give the Combined Company adequate defensive protection or competitive advantages, or that any patents issued to IronNet will not be challenged, invalidated or circumvented. IronNet has filed for patents in the United States and in certain non-U.S. jurisdictions, but such protections may not be available in all countries in which the Combined Company will operate or in which it will seek to enforce intellectual property rights, or the intellectual property rights may be difficult to enforce in practice. For example, many foreign countries have compulsory licensing laws under which a patent owner must grant licenses to third parties under certain circumstances. In addition, many countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. Moreover, the Combined Company may need to expend additional resources to defend its intellectual property rights in these countries, and its inability to do so could impair its business or adversely affect its plans for international expansion. IronNet's currently issued patents and any patents that may be issued in the future with respect to pending or future patent applications may not provide sufficiently broad protection or they may not prove to be enforceable in actions against alleged infringers.

The Combined Company may not be effective in policing unauthorized use of its intellectual property, and even if it does detect violations, litigation may be necessary to enforce its intellectual property rights. Protecting against the unauthorized use of intellectual property rights, technology and other proprietary rights is expensive and difficult, particularly outside of the United States. Any enforcement efforts undertaken, including litigation, could be time-consuming and expensive and could divert management's attention, which could harm the Combined Company's business and results of operations. Further, attempts to enforce rights against third parties could also provoke these third parties to assert their own intellectual property or other rights against the Combined Company, or challenge the intellectual property rights of the Combined Company which could result in a holding that invalidates or narrows the scope of the Combined Company's intellectual property rights, in whole or in part. The inability to adequately protect and enforce its intellectual property and other proprietary rights could seriously harm the Combined Company's business, results of operations and financial condition. Even if it is able to secure its intellectual property rights, we cannot assure you that such rights will provide the Combined Company with competitive advantages or distinguish its services from those of its competitors or that its competitors will not independently develop similar technology, duplicate any of its technology, or design around its patents.

Claims by others that the Combined Company infringes their proprietary technology or other intellectual property rights could result in significant costs and substantially harm its business, financial condition, results of operations and prospects.

Claims by others that the Combined Company infringes or misappropriates their proprietary technology or other intellectual property rights could harm the Combined Company's business. Companies in the cybersecurity industry could hold patents and also protect their copyright, trade secret and other intellectual property rights,

grows and develops the infrastructure of a public operating company, it may be difficult to maintain IronNet's corporate culture. Any failure to preserve that culture could harm the Combined Company's future success, including its ability to retain and recruit personnel, innovate and operate effectively and execute on its business strategy. Additionally, its productivity and the quality of its solutions may be adversely affected if it does not integrate and train new employees quickly and effectively. If the Combined Company experiences any of these effects in connection with future growth, it could impair its ability to attract new customers, retain existing customers and expand their use of IronNet's platform, all of which would adversely affect its business, financial condition and results of operations.

IronNet's international operations and plans for future international expansion expose the Combined Company to significant risks, and failure to manage those risks could adversely impact its business.

IronNet derived 39% and 14% of its total revenue from its international customers for fiscal 2021 and fiscal 2020, respectively. IronNet's growth strategy includes expansion into target geographies, but there is no guarantee that such efforts will be successful. We expect that the Combined Company's international activities will continue to grow in the future, as it continues to pursue opportunities in international markets. These international operations will require significant management attention and financial resources and are subject to substantial risks, including:

- greater difficulty in negotiating contracts with standard terms, enforcing contracts, and managing collections, including longer collection periods;
- higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for international operations and creating international operating entities, where applicable;
- management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of IronNet's platform that may be required in foreign countries;
- greater risk of unexpected changes in applicable foreign laws, regulatory practices, tariffs, and tax laws and treaties;
- compliance with anti-bribery laws, including the U.S. Foreign Corrupt Practices Act of 1977, as amended, the U.S. Travel Act and the UK Bribery Act 2010, violations of which could lead to significant fines, penalties, and collateral consequences;
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;
- the uncertainty of protection for intellectual property rights in some countries;
- general economic and political conditions in these foreign markets;
- foreign exchange controls or tax regulations that might prevent the Combined Company from repatriating cash earned outside the United States;
- political and economic instability in some countries;
- the potential for foreign government demands for access to information or corporate property;
- double taxation of international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which it operates;
- unexpected costs for the localization of services, including translation into foreign languages and adaptation for local practices and regulatory requirements;

The report of IronNet's independent registered public accounting firm included a "going concern" explanatory paragraph.

IronNet has disclosed in its financial statements that it has incurred recurring losses from operations and expects to continue to incur significant costs in pursuit of its next round of financing in fiscal 2022 for capital funding purposes. IronNet has raised substantial doubt about its ability to continue as a going concern. In addition, the report of IronNet's independent registered public accounting firm on its financial statements as of January 31, 2021 and 2020 and for fiscal 2021 and fiscal 2020 included an explanatory paragraph stating that IronNet's recurring losses from operations, combined with its ongoing need to raise additional capital, raised substantial doubt about IronNet's ability to continue as a going concern. IronNet's consolidated financial statements do not include any adjustments that may result from the outcome of this uncertainty and do not reflect the transactions contemplated by the Business Combination. Absent the additional capital from the Business Combination or from an alternative financing if the Business Combination is unsuccessful, IronNet may be unable to continue as a going concern. Future reports from IronNet's independent registered public accounting firm may also contain statements expressing substantial doubt about its ability to continue as a going concern. If such doubt about IronNet continues, investors or other financing sources may be unwilling to provide additional funding to IronNet on commercially reasonable terms, or at all, and IronNet's business may be harmed.

The Combined Company's business will be subject to the risks of natural catastrophic events and to interruption by man-made problems such as power disruptions, computer viruses, data security breaches or terrorism.

A significant natural disaster, such as an earthquake, a fire, a flood, or significant power outage could have a material adverse impact on the Combined Company's business, results of operations and financial condition. Natural disasters could affect its personnel, data centers, supply chain, manufacturing vendors, or logistics providers' ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. In addition, climate change could result in an increase in the frequency or severity of natural disasters. In the event that the Combined Company or its service providers' information technology systems or manufacturing or logistics abilities are hindered by any of the events discussed above, it could result in missed financial targets, such as revenue, for a particular quarter. In addition, computer malware, viruses and computer hacking, fraudulent use attempts and phishing attacks have become more prevalent in the cybersecurity industry, and the Combined Company's internal systems may be victimized by such attacks. Likewise, the Combined Company could be subject to other man-made problems, including but not limited to power disruptions and terrorist acts.

Although the Combined Company will maintain incident management and disaster response plans, in the event of a major disruption caused by a natural disaster or man-made problem, it may be unable to continue its operations and may endure system interruptions, reputational harm, delays in its development activities, lengthy interruptions in service, breaches of data security and loss of critical data, and its insurance may not cover such events or may be insufficient to compensate it for the potentially significant losses it may incur. Acts of terrorism and other geo-political unrest could also cause disruptions in its business or the business of its supply chain, manufacturers, logistics providers, partners, or customers or the economy as a whole. Any disruption in the business of its supply chain, manufacturers, logistics providers, partners or customers that impacts sales at the end of a fiscal quarter could have a significant adverse impact on the Combined Company's financial results. All of the aforementioned risks may be further increased if disaster recovery plans prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, or the delay in the manufacture, deployment, or shipment of the Combined Company's products, its business, financial condition, and results of operations would be adversely affected.

IronNet's management has identified material weaknesses in its internal control over financial reporting and may identify additional material weaknesses in the future or otherwise fail to maintain effective internal control over financial reporting, which may result in material misstatements of the Combined Company's financial statements or cause it to fail to meet its periodic reporting obligations.

As a public company, LGL is required to maintain internal control over financial reporting and to report any material weaknesses in such internal control over financial reporting. IronNet is currently a private company with

limited accounting and financial reporting personnel and other resources with which to address its internal control over financial reporting. In connection with the preparation and audit of IronNet's consolidated financial statements for the year ended January 31, 2021, IronNet and its independent registered public accounting firm identified material weaknesses in its internal control over financial reporting. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of our annual or interim financial statements will not be prevented or detected on a timely basis. IronNet did not have a sufficient number of personnel with an appropriate degree of accounting and internal controls knowledge, experience, and training to appropriately analyze, record and disclose accounting matters commensurate with IronNet's accounting and reporting requirements, which resulted in an inability to consistently establish appropriate authorities and responsibilities in pursuit of its financial reporting objectives. This material weakness contributed to the following additional material weaknesses: IronNet did not design and maintain effective controls over the review of journal entries and account reconciliations. Specifically, certain personnel have the ability to both (i) create and post journal entries within IronNet's general ledger system, and (ii) prepare and review account reconciliations. IronNet did not design and maintain effective controls over information technology ("IT") general controls for information systems that are relevant to the preparation of its financial statements. Specifically, IronNet did not design and maintain: (i) program change management controls for the financial systems to ensure that information technology program and data changes affecting financial IT applications and underlying accounting records are identified, tested, authorized and implemented appropriately; (ii) appropriate user access controls to ensure appropriate segregation of duties and that adequately restrict user and privileged access to financial applications, programs and data to appropriate IronNet personnel; (iii) computer operations controls to ensure data backups are authorized and restorations monitored; and (iv) testing and approval controls for program development to ensure that new software development is aligned with business and IT requirements.

These material weaknesses did not result in a material misstatement to the consolidated financial statements. However, these material weaknesses could result in a misstatement of substantially all accounts or disclosures that would result in a material misstatement to the annual or interim consolidated financial statements that would not be prevented or detected.

With the oversight of senior management, IronNet has instituted plans to remediate these material weaknesses and will continue to take remediation steps, including hiring additional key supporting accounting personnel with public company reporting and accounting operations experience, implementing the required segregation of roles and duties both in manual and systems related processes including for journal entries and account reconciliations, and formalizing the documentation and performance of information technology general controls for information systems utilized for financial reporting.

While IronNet implements its plan to remediate the material weaknesses described above, it cannot predict the success of such plans or the outcome of its assessment of these plans at this time. If its steps are insufficient to remediate the material weaknesses successfully and otherwise establish and maintain effective internal control over financial reporting, the reliability of the Combined Company's financial reporting, investor confidence, and the value of its common stock could be materially and adversely affected. The Combined Company can give no assurance that the implementation of this plan will remediate these deficiencies in IronNet's internal control over financial reporting or that additional material weaknesses or significant deficiencies in its internal control over financial reporting will not be identified in the future. The failure to implement and maintain effective internal control over financial reporting could result in errors in its financial statements that could result in a restatement of its financial statements, causing it to fail to meet its reporting obligations.

Risks Related to an Investment in the Combined Company's Securities

There may not be an active trading market for the Combined Company Common Stock, which may make it difficult to sell shares of the Combined Company Common Stock.

It is possible that after the Business Combination, an active trading market will not develop or, if developed, that any market will not be sustained. This would make it difficult for you to sell shares of the Combined

Company Common Stock at an attractive price or at all. The market price per share of the LGL Common Stock prior to the Business Combination may not be indicative of the price at which shares of the Combined Company Common Stock will trade in the public market after the Business Combination.

The market price of shares of the Combined Company Common Stock may be volatile, which could cause the value of your investment to decline.

Even if an active trading market develops following the Business Combination, the market price of the Combined Company Common Stock may be highly volatile and could be subject to wide fluctuations. Securities markets worldwide experience significant price and volume fluctuations. The securities markets have experienced significant volatility as a result of the COVID-19 pandemic. Market volatility, as well as general economic, market or political conditions, could reduce the market price of shares of the Combined Company Common Stock regardless of its operating performance. The Combined Company's operating results could be below the expectations of public market analysts and investors due to a number of potential factors, including:

- variations in quarterly operating results or dividends, if any, to stockholders;
- additions or departures of key management personnel;
- publication of research reports about the Combined Company's industry;
- litigation and government investigations;
- changes or proposed changes in laws or regulations or differing interpretations or enforcement of laws or regulations affecting the Combined Company's business;
- adverse market reaction to any indebtedness incurred or securities issued in the future;
- changes in market valuations of similar companies;
- adverse publicity or speculation in the press or investment community;
- announcements by competitors of significant contracts, acquisitions, dispositions, strategic partnerships, joint ventures, or capital commitments; and
- the impact of the COVID-19 pandemic (or future pandemics) on the Combined Company's management, employees, partners, customers, and operating results.

In response to any of the foregoing developments, the market price of shares of the Combined Company Common Stock could decrease significantly. You may be unable to resell your shares at or above your purchase price.

Following periods of volatility in the overall market and the market price of a company's securities, securities class action litigation has often been instituted against that company. Any such litigation, if instituted against the Combined Company, could result in substantial costs and a diversion of management's attention and resources.

A small number of stockholders will continue to have substantial control over the Combined Company after the Business Combination, which may limit other stockholders' ability to influence corporate matters and delay or prevent a third party from acquiring control over the Combined Company.

Upon completion of the Business Combination, the directors and executive officers of the Combined Company, and beneficial owners expected to own 5% or more of its voting securities and their respective affiliates, will beneficially own, in the aggregate, approximately % of its outstanding common stock, assuming no Public Stockholders redeem their LGL common stock. This significant concentration of ownership may have a negative impact on the trading price for the Combined Company Common Stock because investors often perceive disadvantages in owning stock in companies with controlling stockholders. In addition, these stockholders will be able to exercise influence over all matters requiring stockholder approval, including the election of directors and approval of corporate transactions, such as a merger or other sale of the Combined

Company or its assets. This concentration of ownership could limit stockholders' ability to influence corporate matters and may have the effect of delaying or preventing a change in control, including a merger, consolidation or other business combination, or discouraging a potential acquirer from making a tender offer or otherwise attempting to obtain control, even if that change in control would benefit the other stockholders.

There can be no assurance that the Combined Company's securities will be approved for listing on the NYSE or that the Combined Company will be able to comply with the continued listing standards of the NYSE.

In connection with the Business Combination, we intend to list the common stock and warrants of the Combined Company on the NYSE under the symbols "IRNT" and "IRNTW," respectively. The Combined Company's continued eligibility for listing may depend on the number of shares of LGL common stock that are redeemed. If, after the Business Combination, NYSE delists the Combined Company's securities from trading on its exchange for failure to meet the listing standards, the Combined Company and its stockholders could face significant negative consequences, including:

- limited availability of market quotations for the Combined Company's securities;
- a determination that the Combined Company Common Stock is a "penny stock," which would require brokers trading in the common stock to adhere to more stringent rules;
- possibly resulting in a reduced level of trading activity in the secondary trading market for shares of the Combined Company Common Stock;
- a limited amount of analyst coverage; and
- the decreased ability to issue additional securities or obtain additional financing in the future.

If the Combined Company's operating and financial performance in any given period does not meet the guidance provided to the public or the expectations of investment analysts, the market price of its common stock may decline.

The Combined Company may, but is not obligated to, provide public guidance on its expected operating and financial results for future periods. Any such guidance will consist of forward-looking statements, subject to the risks and uncertainties described in this prospectus/proxy statement and in the Combined Company's other public filings and public statements. The ability to provide this public guidance, and the ability to accurately forecast its results of operations, could be impacted by the COVID-19 pandemic. The Combined Company's actual results may not always be in line with or exceed any guidance it has provided, especially in times of economic uncertainty, such as the current global economic uncertainty being experienced as a result of the COVID-19 pandemic. If, in the future, the Combined Company's operating or financial results for a particular period do not meet any guidance provided or the expectations of investment analysts, or if the Combined Company reduces its guidance for future periods, the market price of the Combined Company Common Stock may decline as well. Even if the Combined Company does issue public guidance, there can be no assurance that it will continue to do so in the future.

Following the consummation of the Business Combination, the Combined Company will incur significant increased expenses and administrative burdens as a public company, which could negatively impact its business, financial condition and results of operations.

Following the consummation of the Business Combination, the Combined Company will face increased legal, accounting, administrative and other costs and expenses as a public company that IronNet has not historically incurred as a private company. The Sarbanes-Oxley Act of 2002, or Sarbanes-Oxley, including the requirements of Section 404(a) relating to disclosing (i) management's responsibility for establishing and maintaining internal control over financial reporting and (ii) annually assessing the effectiveness of the internal control over financial reporting, as well as rules and regulations subsequently implemented by the SEC, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 and the rules and regulations promulgated

and to be promulgated thereunder, the PCAOB and the securities exchanges, impose additional reporting and other obligations on public companies. Compliance with public company requirements will increase costs and make certain activities more time-consuming.

A number of these requirements will require the Combined Company to carry out activities that IronNet has not done previously. For example, the Combined Company will create new board committees and adopt new internal controls and disclosure controls and procedures. In addition, expenses associated with SEC reporting requirements will be incurred. Furthermore, if any issues in complying with those requirements are identified (for example, if the Combined Company identifies a material weakness or significant deficiency in the internal control over financial reporting), the Combined Company could incur additional costs rectifying those issues, and the existence of those issues could harm the Combined Company's reputation or investor perceptions of it. It may also be more expensive to obtain director and officer liability insurance. Risks associated with the Combined Company's status as a public company may make it more difficult to attract and retain qualified persons to serve on the board of directors of the Combined Company (the "*Combined Company Board*") Board or as executive officers. The additional reporting and other obligations imposed by these rules and regulations will increase legal and financial compliance costs and the costs of related legal, accounting and administrative activities. These increased costs will require the Combined Company to divert a significant amount of money that could otherwise be used to expand the business and achieve strategic objectives. Advocacy efforts by stockholders and third parties may also prompt additional changes in governance and reporting requirements, which could further increase costs.

If the Combined Company is unable to implement and maintain effective internal control over financial reporting in the future, investors may lose confidence in the accuracy and completeness of financial reports, and the market price of its common stock may decline.

The Combined Company will be required to maintain internal control over financial reporting and to report any material weaknesses in such internal controls. In addition, following the Business Combination, it will be required to furnish a report by management in its annual report on Form 10-K on the effectiveness of its internal control over financial reporting, pursuant to Section 404 of Sarbanes-Oxley. The process of designing, implementing, and testing the internal control over financial reporting required to comply with this obligation is time-consuming, costly, and complicated. If the Combined Company identifies material weaknesses in its internal control over financial reporting, if it is unable to comply with the requirements of Section 404 of Sarbanes-Oxley in a timely manner, or if it is unable to assert that its internal control over financial reporting are effective, it will be unable to certify that its internal control over financial reporting is effective. The Combined Company cannot assure you that there will not be material weaknesses or significant deficiencies in its internal control over financial reporting in the future. Any failure to maintain internal control over financial reporting could severely inhibit the Combined Company's ability to accurately report its financial condition or results of operations. If it is unable to conclude that its internal control over financial reporting is effective, investors may lose confidence in the accuracy and completeness of the Combined Company's financial reports and the market price of the Combined Company Common Stock could decline. The Combined Company could become subject to investigations by the NYSE, the SEC or other regulatory authorities, which could require additional financial and management resources.

The Combined Company will qualify as an "emerging growth company." The reduced public company reporting requirements applicable to emerging growth companies may make its common stock less attractive to investors.

Following the consummation of the Business Combination, the Combined Company will qualify as an "emerging growth company" under SEC rules. As an emerging growth company, the Combined Company will be permitted and plans to rely on exemptions from certain disclosure requirements that are applicable to other public companies that are not emerging growth companies. These provisions include, but are not limited to: (1) an exemption from compliance with the auditor attestation requirement in the assessment of internal control over financial reporting pursuant to Section 404 of Sarbanes-Oxley, (2) not being required to comply with any requirement that may be adopted by the PCAOB regarding mandatory audit firm rotation or a supplement to the

auditor's report providing additional information about the audit and the financial statements, (3) reduced disclosure obligations regarding executive compensation arrangements in periodic reports, registration statements, and proxy statements, and (4) exemptions from the requirements of holding a nonbinding advisory vote on executive compensation and stockholder approval of any golden parachute payments not previously approved. Further, Section 102(b)(1) of the JOBS Act exempts emerging growth companies from being required to comply with new or revised financial accounting standards until private companies (that is, those that have not had a Securities Act registration statement declared effective or do not have a class of securities registered under the Exchange Act) are required to comply with the new or revised financial accounting standards. The JOBS Act provides that a company can elect to opt out of the extended transition period and comply with the requirements that apply to non-emerging growth companies but any such election to opt out is irrevocable. As a result, the information the Combined Company provides will be different than the information that is available with respect to other public companies that are not emerging growth companies. If some investors find the Combined Company Common Stock less attractive as a result, there may be a less active trading market for the Combined Company Common Stock, and the market price of the Combined Company Common Stock may be more volatile.

IronNet's management has limited experience in operating a public company.

IronNet's executive officers have limited experience in the management of a publicly traded company. IronNet's management team may not successfully or effectively manage its transition to a public company that will be subject to significant regulatory oversight and reporting obligations under federal securities laws. Their limited experience in dealing with the increasingly complex laws pertaining to public companies could be a significant disadvantage in that it is likely that an increasing amount of their time may be devoted to these activities, which will result in less time being devoted to the management and growth of the Combined Company. IronNet may not have adequate personnel with the appropriate level of knowledge, experience, and training in the accounting policies, practices or internal control over financial reporting required of public companies in the United States. The development and implementation of the standards and controls necessary for the Combined Company to achieve the level of accounting standards required of a public company in the United States may require costs greater than expected. It is possible that the Combined Company will be required to expand its employee base and hire additional employees to support its operations as a public company, which will increase its operating costs in future periods.

If securities or industry analysts do not publish research or reports about the Combined Company's business or publish negative reports, the market price of its common stock could decline.

The trading market for the Combined Company Common Stock will be influenced by the research and reports that industry or securities analysts publish about the Combined Company or its business. If regular publication of research reports ceases, the Combined Company could lose visibility in the financial markets, which in turn could cause the market price or trading volume of the Combined Company Common Stock to decline. Moreover, if one or more of the analysts who cover the Combined Company downgrade its common stock or if reporting results do not meet their expectations, the market price of the common stock could decline.

If the Combined Company's security holders exercise their registration rights, it may negatively impact the market price of the Combined Company Common Stock.

In connection with the Business Combination, LGL's existing registration rights agreement will be amended and restated to: (i) provide that the Combined Company will file a registration statement following the closing of the Business Combination to register for resale (A) certain of the shares of LGL common stock outstanding prior to the Business Combination or issuable upon exercise of the Private Warrants held by the Sponsor, (B) certain of the shares of the Combined Company Common Stock to be issued to the IronNet stockholders in the Business Combination and (C) the shares of LGL common stock to be issued in connection with the Private Placement; and (ii) afford each such party "piggyback" registration rights with respect to any underwritten offerings by the other stockholders and by the Combined Company. The sale or possibility of sale of these additional securities trading in the public market may negatively impact the market price of the Combined Company's securities.

- Competitive Relationship—The risk of one company directly assisting its competitor through participation in a collective defense scheme (e.g., AT&T assisting Verizon, or General Motors assisting Toyota) cannot be ignored. The legal and marketing teams from participating organizations would be wise to adopt the airline and energy industry's observations that a mutual focus on safety helps every participant.

The benefits and risks of cooperation for large-scale cybersecurity across heterogenous groups must be carefully balanced in setting up a collective defense. Too often, collectives are developed that leave participants wondering what's in it for them, and how potential problems might be avoided. One main value proposition from IronNet is that cooperative cybersecurity will work best when such concerns are carefully curated by a trusted provider with a world-class platform.

Role of Government in Collective Defense

One challenge federal governments have in supporting collective cyber defense is that most large businesses are multi-national. This suggests that while national allegiance might be easily identified (e.g., Verizon is American, Huawei is Chinese), such allegiance must address the interests of the company's shareholders. This emphasis is often misunderstood by government agencies who are focused exclusively on national interests.

Federal governments also have the additional role to regulate and sometimes punish organizations not meeting their security requirements. This obligation complicates government cooperation with business on cybersecurity, at least to the extent that governments are permitted to regulate based on voluntarily shared information. Organizations would thus be hesitant to share information with a cooperative involving government if the reported incident might lead to regulatory investigation.

The biggest challenge, however, is that the majority of critical infrastructure is owned and operated by the private sector. This implies that security telemetry, indicators, and early warnings will come from the private sector, even for many military applications and defensive government activities. This fact is often not understood by citizens and politicians who may demand that government step in and fix large-scale cybersecurity threats. This is usually just not practically feasible.

Government must work hard to share the information it uniquely controls, such as classified indicators that might be downgraded for sharing externally or be shared in a more limited context to defend critical infrastructure. Businesses must also recognize that their obligations extend beyond just the shareholder. This recognition that cooperative sharing is in the best interests of the organization and society in general is an important driver behind IronNet's platform offering.

Overview of IronNet's Platform Offering

The Collective Defense platform comprises two flagship products:

IronDefense is an advanced Network Detection and Response ("*NDR*") solution that uses AI-driven behavioral analytics to detect and prioritize anomalous activity inside individual enterprises. IronNet leverages advanced Artificial Intelligence/Machine-Learning ("*AI/ML*") algorithms to detect previously unknown threats that have not been identified and "fingerprinted" by industry researchers), in addition to screening any known threats, and applies its Expert System to prioritize the severity of the behaviors—all at machine speed and cloud scale.

IronDome is a threat-sharing solution that facilitates a crowdsource-like environment in which the IronDefense threat detections from an individual company are shared among members of a Collective Defense community, consisting of IronNet customers who have elected to permit their information to be anonymously shared and cross-correlated by IronNet's IronDome systems. IronDome analyzes threat detections across the

community to identify broad attack patterns and provides anonymized intelligence back to all community members in real time, giving all members early insight into potential incoming attacks. Automated sharing across the Collective Defense community enables faster detection of attacks at earlier stages.

IronNet's Collective Defense platform is designed to deliver strong network effects. Every customer contributing its threat data (anonymously) into the community is able to reap benefits from the shared intelligence of the other organizations. The collaborative aspect of Collective Defense, and the resulting prioritization of alerts based on their potential severity, helps address the known problem of "alert fatigue" that plagues overwhelmed security analysts.

The Collective Defense platform is available for on-premise, cloud (public or private), and hybrid environments, and is scalable to include small-to-medium businesses and public-sector agencies as well as multinational corporations. IronNet provides professional cybersecurity services such as incident response and threat hunting, as well as programs to help customers assess cybersecurity governance, maturity, and readiness. IronNet's CS services are designed to create shared long-term success measures with its customers, differentiating it from other cybersecurity vendors by working alongside customers as partners and offering consultative and service capabilities beyond implementation.

The Collective Defense platform is available via a subscription-based pricing and flexible delivery model, with options available for major public cloud providers such as Amazon Web Services and Microsoft Azure; private cloud, or Hyper Converged Infrastructure ("*HCI*") such as Nutanix; and on-premise environments through hardware and virtual options. To make it as easy as possible for customers to add Collective Defense into their existing security stack, IronNet built a rich set of Application Programming Interfaces ("*APIs*") that enable integrations with standard security products, including security information and event management ("*SIEM*"); security orchestration, automation, and response ("*SOAR*"); endpoint detection and response ("*EDR*"); next-generation firewall ("*NGFW*") tools; and cloud-native logs from the major public cloud providers.

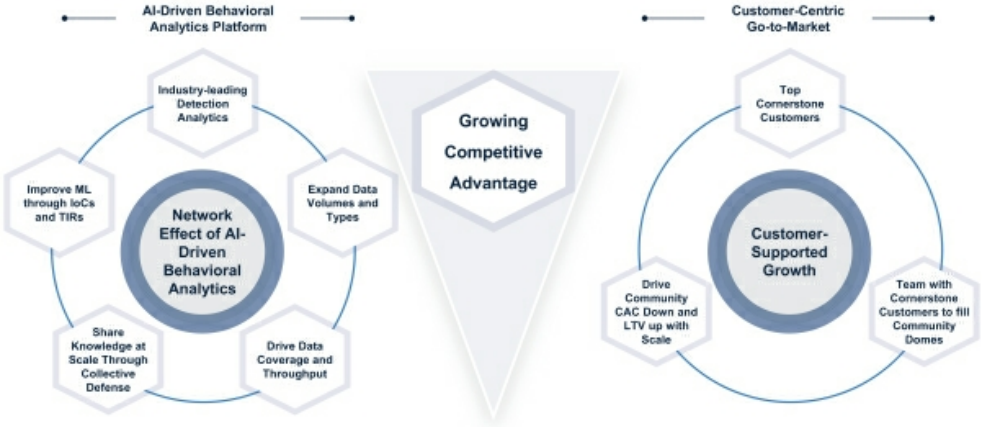
IronNet describes its go-to-market strategy as "land and expand with network effects." Its approach is to initially secure influential "cornerstone" customers and then expand into their respective Collective Defense communities with additional "community members" from organizations of similar industry sector, state, country, supply chain, or tailored business ecosystem. As each Collective Defense community grows, so does the volume of shared data, and the value of IronNet's platform for each of those members thereby expands both technically and commercially.

IronNet sells into both public and private organizations and the business ecosystems that support them. IronNet has identified tens of thousands of prospective cornerstone customers and more than 100,000 potential community customers.

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust IronNet to protect their networks. IronNet's customers include a top global hedge fund, eight of the top 10 U.S. energy companies (based on revenue), a leading Asian mobile phone carrier, two U.S. Department of Defense ("*DoD*") branches, a mid-sized bank in the EMEA region, four U.S. state agencies, U.K. and Singapore government entities, and a large global holding company.

IronNet began targeting large enterprises and Fortune 500 companies, but the flexibility and scalability of its cloud-native platform and enhanced go-to-market approach enabled it to expand its customer base to smaller companies as well. IronNet has been recognized in the cybersecurity industry by independent third-party analysts, including Gartner, Forrester, IDC, 451 Research Group, and Omdia, who has called IronNet's analytics a "potential game changer" in a June 2020 report. In January 2021, the global insurance brokerage Marsh named the Collective Defense platform as one of its industry-recognized Cyber Catalyst solutions. In August 2020, IronNet announced that it had achieved "FedRAMP-ready" for Agency Authorization status, as approved by the Federal Risk and Authorization Management Program (FedRAMP).

The overall effect of its go-to-market approach drives two powerful network effects, which are depicted in the graphic below. The first is the growth in the value of IronNet's platform as it ingests more and different data to improve the detection of its machine learning-driven algorithms. The second is its customer community-driven growth model, which drives a more efficient route to market with lower community customer acquisition costs and higher customer lifetime values.



IronNet's Growth Strategy

IronNet sees the opportunity for multi-dimensional innovation and growth. IronNet believes that the SolarWinds/SUNBURST attack in 2020 has validated its mission to drive AI-driven behavioral analytics and Collective Defense to the overall security market.

IronNet's revenues have grown steadily since its first product release in 2016. It made its first moves to the cloud in 2018, and it intends to accelerate scalability from its cloud offerings. This evolution in IronNet's products allow it to deploy to customers more rapidly, scale more quickly, and drive revenue growth.

IronNet's strategies to grow its business include the following:

Grow its customer base by replacing legacy and other NDR products

Given the limitations of existing products in the NDR, SIEM, IDPS, EDLP, and Threat Intelligence Software segments, IronNet intends continue to grow its customer base organically as organizations replace these signature-based and stand-alone offerings with AI-driven behavioral analytics and Collective Defense. Its customer acquisition campaigns and channel partnerships with MDR providers are expected to allow IronNet to pair pursuit of large enterprise customers with cost-effective penetration into smaller and medium-sized enterprises.

Further expand offerings with existing customers

IronNet will continue to expand its relationships with its customers by expanding its network coverage of their business towards 100% and by cross-selling additional Collective Defense offerings. When IronNet first deploys its products to a customer, it usually covers only a portion of their network traffic. As IronNet is able to demonstrate the value of its behavioral analytics and membership in Collective Defense, it has up-sell

opportunities as it expands network coverage to other parts of the business or portfolio. IronNet also has the opportunity to cross-sell offerings like cloud traffic analytics or digital fraud detection. Over time, IronNet seeks to deploy its solutions enterprise-wide for all customers, thereby increasing its revenue from existing customers and therefore its dollar-based net retention rates.

Expand into new customer segments

While IronNet first targeted large and sophisticated enterprise customers, it also has an internal sales development team and an inside sales team to expand its go-to-market efforts. These teams focus on early qualification and development for cycles with potential cornerstone customers. They utilize intelligence from IronNet's Account Based Marketing system as well as social sales development tools to nurture these opportunities to a handoff point with field sales. These teams also focus on full cycles with potential community members once a cornerstone-driven Collective Defense community has been established. IronNet is using a combination selling approach to scale its sales into additional industry verticals, with which it can sell its Collective Defense capabilities to the largest enterprises or smallest businesses with any level of security sophistication and budget.

Extend its Collective Defense platform and ecosystem

IronNet designed its architecture to be open, interoperable, and highly extensible. It is constantly adding integrations to its platform in order to ingest more sources of data for analysis and to provide detection outputs to more response systems. IronNet also adds new algorithms and new combinations of algorithms to detect behaviors of unknown but potentially malicious attacks. In addition, IronNet innovates with partners to add IronNet NDR and Collective Defense capabilities to their customer offerings. An example of this is IronNet's recent announcement of a strategic partnership with Jacobs Engineering Group, an international technical professional services firm, under which the parties will work together to develop an end-to-end solution designed to detect and prevent damaging and difficult-to-detect cyberattacks that continue to plague organizations across public and private sectors. The joint offering of Jacobs' managed services capabilities and IronNet's advancements in machine learning and AI provides their respective customers a more thorough approach to network security. IronNet expects that innovations and partnerships such as its partnership with Jacobs will enhance the distribution of its platform and represent future sources of revenue.

Broaden reach into the U.S. federal government vertical

IronNet spent the first five years of its life building foundational customer relationships in the commercial sector. This was intentional, as its company mission required it first to build the technology and business basis required to protect the private side of the public/private partnership. IronNet is now actively investing in the acquisition of customers in the U.S. federal government vertical. IronNet is FedRAMP Ready and is registered with the Department of Homeland Security Continuous Diagnostics & Monitoring program approved products list to provide federal agencies with innovative security tools. In addition, its platform is deployed in the AWS GovCloud. IronNet is pursuing opportunities in the civilian, defense, and intelligence sectors.

Expand its international footprint

IronNet is expanding its international operations and will continue to invest globally to broaden its international footprint. IronNet intends to grow its presence in the Asia Pacific Japan and EMEA regions by adding headcount and establishing overseas hosting relationships.

vendors charge a premium for expert Customer Success care, IronNet includes access to its CS team as part of a customer's subscription, including a dedicated Customer Success Manager for the life of the subscription.

At the onset of a new deployment, IronNet's CS team works with customer stakeholders to map out what success looks like, determine the key deliverables required to achieve those goals and create a success plan for the life of the partnership.

Governance and Maturity Services

These services measure adherence to specific regulatory or contractual requirements and provide measurable data as to the maturity of the organization's cybersecurity capabilities.

Cybersecurity Readiness Services

Given that threat actors continuously change their tactics, techniques, and procedures ("*TTP*"), these services are designed to ensure organizations are prepared for the latest and most immediate threats.

Incident Response Services

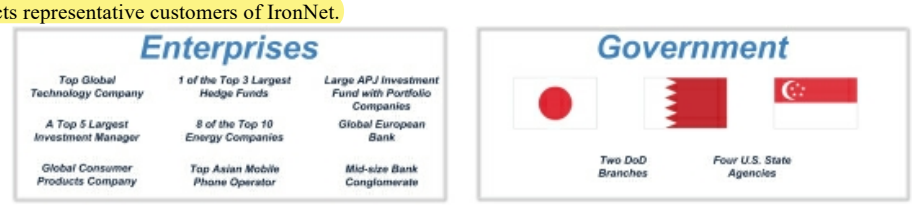
IronNet provides incident response and digital forensic investigative services powered by an accomplished team with deep expertise. IronNet specializes in providing incident response and digital forensic investigative services to companies of all sizes, ranging from large U.S. Fortune 50 companies to smaller organizations.

Training

Leveraging decades of cybersecurity experience, IronNet's results-focused training programs enable customers to unlock a higher level of cyber resilience. IronNet adopts a hands-on approach to build technical proficiency and operational confidence using industry best practices. Cyber skillset training techniques include hunt methodology, offensive methodology, data analytics for security intelligence, SOC leadership, cyber threat intelligence operations, executive education, and custom cyber threat seminars.

IronNet's Customers

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust IronNet to protect their networks. The following graphic depicts representative customers of IronNet.



Customer case studies

Critical infrastructure customer case study: Southern Company

Within IronNet's first months in business, it had five major utility companies sharing cyber events in the IronDome across 25 states, helping secure infrastructure that delivers power to nearly 35 million customers.

Situation: Serving nine million customers across six states, Southern Company faced risks as a target for cyber attackers to steal information or disrupt operations.

Solution: As an early adopter of Collective Defense, one of the reasons Southern Company works with IronNet is to get high quality, automated situational awareness and to move away from relying on manual methods. Southern Company invested in its partnership with IronNet to increase its ability to detect Advanced Persistent Threats, reduce dwell time and more quickly recover in the event of an attack.

IronNet's relationship with Southern Company extends beyond just a vendor/client relationship, as senior leadership from both companies appear together at numerous events and government briefings to discuss their positions on topics like nuclear energy and the security of the U.S. power grid.

Southern Company's Chief Information Security Officer notes that "Broad situational awareness within sectors and across sectors is something we believe in, and why we are doing work with IronNet and many other partners in energy and other critical sectors, both nationally and internationally."

Critical infrastructure case study: American Electric Power (AEP)

Situation: With the nation's largest transmission system consisting of more than 40,000 miles of transmission lines and more extra-high-voltage transmission lines than all other companies combined in North America, AEP needed to ensure the security of its own operations—while recognizing its role in contributing to the security of the electrical grid overall. collaborative cyber defense to combat adversaries.

Solution: Collective Defense provides the high-fidelity threat sharing to make AEP's cyber intelligence truly actionable, to ensure the cyber security of its 5.5 million customers.

AEP's Chief Security Officer says that "AEP values the relationship and initiatives being led by Gen. Alexander and IronNet."

Financial services customer case study: NBH Bank

Situation: National Bank Holdings ("*NBH"*) needed a way to detect unknown threats. Monitoring only known threats, or "signatures" such as compromised domain names, IP addresses, or file hashes, missed a huge swath of threats that evade traditional signature-based threat detection. NBH needed a tool that could alert the security team of advanced threats across the cyber kill chain, in real time, in turn empowering the team to take action before the threat could affect operations.

Solution: After evaluating other platforms, NBH chose IronDefense for its ability to successfully detect malicious behaviors for DNS Tunneling, Domain Generation Algorithm (DGA), and Periodic Beaconing HTTP. As part of an IronDome, NBH has strengthened its ability to take proactive action against emerging threats detected by machine learning and further qualified by anonymized knowledge-sharing in the Collective Defense ecosystem.

NBH selected IronNet because of its precise analytics; proactive hunt team support; partnership with IronNet's Customer Success team; and the ability to crowdsource expertise across their peers through Collective Defense.

NBH's VP of Enterprise Technology has stated that it views IronNet's Collective Defense as the "next big thing in cyber."

Sovereign wealth fund customer case study

Situation: An Asia-Pacific-based sovereign wealth fund with a $300 billion portfolio needed better visibility of network threats across its portfolio companies. Prior to implementing Collective Defense, neither the sovereign wealth fund nor its portfolio companies had a viable method for correlating IoCs across multiple organizations. They also lacked the ability to detect malicious threat activity based on network behaviors.

Solution: The company chose a Collective Defense IronDome to reduce time to detection via threat sharing across its portfolio companies.

In one instance, IronNet analytics detected a sinister BotNet intrusion attempt into the firm's perimeter. The detection allowed the firm to act fast and catch the BotNet on their firewall before it got inside their network – all within 24 hours of detection.

The fund's Chief Technology Officer said that "None of our other threat hunting tools sparked an alarm. This may suggest that we can turn off some of our other threat hunting tools and save some money by using IronNet. This is IronNet value at work"

In addition to becoming an IronNet customer, the sovereign wealth fund also later became an investor in IronNet.

Oil & gas customer case study

Situation: A Fortune 500 midstream natural gas and crude oil pipeline company sought to increase its detection capabilities and accelerate threat response. Other methods of information sharing proved challenging for driving real business value.

Solution: IronDome provides visibility across the sector and an instantaneous way to share anonymized threat information, allowing the company to identify unknown threats faster and react more quickly. Based on network behavior, IronNet's detection analytics help the company to maximize the value of its other cybersecurity investments by identifying potential misconfigurations or gaps to tighten overall security.

According to the company's leader of Security Operations, "IronNet is truly a partner and not just another vendor."

IronNet's Sales and Marketing

Sales

IronNet uses a "to and through" sales strategy. By maintaining a direct sales force consisting of senior-level account executives with deep security and high-tech experience, IronNet has been able to leverage extensive professional networks and build inroads to strategic accounts. Because of this and the caliber of its senior leadership team, IronNet believes it has a differentiated ability to convene CEOs, Chief Information Security Officers (CISOs) and other leaders within an entire industry, such as energy company CEOs. This is what enables its cornerstone/community selling approach.

IronNet has three sales teams in the United States: Public Sector, covering federal, state and local segments; Critical Infrastructure, covering energy, oil & gas, and related segments; and Enterprise, covering financial services, insurance, tech, and a variety of other sectors. IronNet has direct sales staff in six countries, as well as a growing portfolio of channel, managed services and technology partners across the United States, Europe, Middle East and Africa (EMEA) and Asia-Pacific regions to scale its ability to discover, qualify, and close business.

In addition, IronNet has inside sales development teams to expand its selling capabilities. These teams focus on early qualification and development of opportunities that they either close directly or transition to the field sales teams (for named accounts). These inside teams' primary objective is filling Collective Defense communities with smaller companies.

Marketing

IronNet's marketing organization employs high-tech multichannel digital and content marketing for lead generation, aggressive public relations, social media and thought leadership programs to drive awareness, and specialization in strategies such as employee advocacy and search engine optimization. IronNet was recently the top organic search engine result for "Network Detection and Response" in a competitive market.

IronNet's public relations and media program has resulted in regular coverage in business press, cybersecurity trade media and industry trade media.

IronNet's event program is focused on exposure to audiences that are aligned to its sales strategy. IronNet incorporates a combination of both large industry events like Black Hat with regional and sector-focused events that allow it to capture leads on new customers to build out Collective Defense communities. Immediately at the onset of the COVID-19 pandemic, IronNet pivoted its in-person event plan and launched a program of more than 40 webinars over the past 12 months with industry thought leaders. IronNet also regularly hosts customers on its webinars as a strategic way to create customer case studies from transcripts.

IronNet focuses on providing compelling content for both demand generation and awareness-building. Its monthly Threat Intelligence Briefs summarize the IOCs and detections its SOC has discovered in order to inform the efforts of other operations analysts in the cybersecurity space. IronNet's threat researchers produce in-depth analysis on topics such as ransomware detection and unique technical observations about the SUNBURST attack and other topics, which have been featured in media outlets. This helps build credibility with the security analyst audience, a key influencer in the buying process.

IronNet's Partnership Ecosystem

The IronNet partner ecosystem consists of leading organizations that have been carefully selected to help it deliver the power of Collective Defense across a variety of dimensions.

Technology partners

When used together, IronNet's partner integrations leverage its collective threat intelligence to react in real time, as well as proactively combat threats across the entire network, and create workflows that mitigate compromised devices. IronNet's integrations are designed to increase the efficiency of security teams with smarter, more effective workflows built through collective threat intelligence. To streamline the alert triage and incident response processes, IronDefense can integrate with a number of security products, including:

- SIEM tools to retrieve logs, share detections, and retrieve analyst feedback;
- SOAR tools to share detections, retrieve analyst feedback, and augment existing playbooks;
- EDR platforms to ingest endpoint event and entity context and initiate response to malicious activity; and
- NGFW products to dynamically block malicious activity and ingest logs for analysis.

Current and planned future integrations and APIs include:

Cloud
- AWS
- Azure
- GCP

SIEM
- Splunk
- IBM QRadar
- Microsoft Azure Sentinel
- LogRhythm

SOAR
- Cortex XSOAR (formerly Demisto)
- Splunk Phantom
- Swimlane

ITSM
- ServiceNow

EDR
- CrowdStrike
- Carbon Black
- Forescout
- Tanium

NGFW
- Palo Alto Networks
- Checkpoint Software Technologies
- Zscaler

Go To Market (GTM) Partners

With its GTM partners, IronNet seeks to accelerate service growth and value for their customers through a mutually beneficial program.

Raytheon Technologies

This partnership delivers cybersecurity solutions that defend against advanced threats that leverage behavior-based network traffic analysis and collective defense. The Raytheon-IronNet partnership combines IronNet's Collective Defense Platform with Raytheon's Managed Security Operations Center ("*MSOC*"), Managed Detection and Response ("*MDR*") and Cyber Security Operations Center ("*CSOC*") capabilities. This partnership delivers new analytical solutions that strengthen enterprise protection, along with a customized onboarding to integrate and operate the platform.

Accenture

IronNet and Accenture work together to help companies protect critical infrastructure by quickly deploying and updating a system of machine-speed, advanced threat analytics across IT and Operational Technology, which automatically filters out the noise of false positives with the insight provided by community sourced context. Accenture provides the expertise in scalable implementation when it orchestrates the IronNet collective defense platform, delivering actionable attack information in real-time for their customers to prevent impact to critical infrastructure.

MDR/MSSP partners

Chosen channel partners work with IronNet to develop and deliver an end-to-end solution designed to detect and prevent damaging and difficult-to-detect cyberattacks that continue to plague organizations across public and private sectors. For example, Jacobs' partnership with IronNet brings together unique capabilities, helping customers to navigate the complexities of the current threat landscape more easily. Jacobs provides a full spectrum of professional services including consulting, technical, scientific and project delivery for the government and private sector. The joint offering of Jacobs and IronNet collective defense platform brings advancements in machine learning and AI, which provides innovative cyber defense detection to discover both known and unknown cyber threats, allowing a more thorough and effective approach to network security for their clients.

IronNet's other integration and sales partners include Atlantic Data Forensics, Blacklake Security, Booz Allen Hamilton, Unlimited Technology, ArmorText, Carahsoft, Domain Tools, Ensign Infosecurity, Forescout and Global Cyber Alliance.

IronNet's Research and Development

IronNet's Engineering and Product Development teams are responsible for the architecture and implementation of its Collective Defense platform. Its team of data scientists, data engineers, and emerging threat researchers work together to continually improve the analytics which drive IronDefense. IronNet's Cloud Infrastructure and Sensor teams are dedicated to making IronDome sustained reliability, and scalable on premises and in the cloud.

IronNet is built upon innovations in cybersecurity technology, delivering continuous improvement in detection and mitigation of threats. Its expertise and history in defense and cybersecurity brings a holistic point of view to the design of its solutions, allowing it to find novel threats and share them in real time. IronNet focuses investment on research into emerging threats and advanced data science to keep its Collective Defense platform at the forefront of the most dangerous security issues. IronNet uses feedback from its customers and channel

- maintains and improves operational, financial, and management information systems;
- hires additional personnel;
- obtains, maintains, expands, and protects its intellectual property portfolio; and
- enhances internal functions to support its operations as a publicly-traded company.

Impact of COVID-19 On Our Business

In December 2019, the first cases of COVID-19 were reported in China. In March 2020, the World Health Organization declared COVID-19 a global pandemic. We operate in geographic locations that have been impacted by COVID-19. The pandemic has impacted, and could further impact, our operations and the operations of our customers as a result of quarantines, various local, state and federal government public health orders, facility and business closures, and travel and logistics restrictions. We anticipate governments and businesses will likely take additional actions or extend existing actions to respond to the risks of the COVID-19 pandemic. We are continuing to actively monitor the impacts and potential impacts of the COVID-19 pandemic on our customers, supply chain, and other integral parts of our operations.

We instituted a global work-from-home policy in March 2020 and to date have not experienced significant disruptions as a result. We expect that most of our employees will work from home indefinitely. As part of our shift to remote operations, we terminated several office leases that did not have a material financial impact on us.

In response to the increased economic uncertainties that the impact of the COVID-19 pandemic may have on our business, results of operations and liquidity and capital resources, we took measures to ensure that we would be able to maintain the continuity of our business operations. For example, in April 2020 we obtained a loan in the amount of $5.6 million from the U.S. Small Business Administration (SBA) under the Paycheck Protection Program (PPP). No payments are due under the loan until August 2021. Although we believe we remain eligible to request forgiveness of the loan amount under the rules of the SBA, we have no current intention to do so. In addition to receiving a PPP loan under the CARES Act, we also elected to defer our portion of payroll taxes due for the period from March 2020 through December 31, 2020. Of the deferred amounts, one-half will become due on each of December 31, 2021 and 2022.

Key Factors Affecting Performance

New customer acquisition

Our future growth depends in large part on our ability to acquire new customers. If our efforts to attract new customers are not successful, our revenue may decline in the future. Our IronDefense and IronDome platforms are designed to be used in conjunction with point solutions to capture and share critical data and findings to enable our behavioral analytics to identify threats and for defenders to respond more accurately and quickly. IronNet believes that it has significant room to capture additional market share and intends to continue to invest in sales and marketing to engage its prospective customers, increase brand awareness, and drive adoption of its solution.

Customer retention

Our ability to increase revenue depends in large part on our ability to retain existing customers.

Investing in business growth

Since inception, we have invested significantly in the growth of our business. We intend to continue to invest in our research and development team to lead product improvements, our sales team to broaden our brand

awareness and our general and administrative expenses to increase for the foreseeable future given the additional expenses for finance, compliance and investor relations as we grow as a public company. In addition to our internal growth, we may also consider acquisitions of businesses, technologies, and assets that complement and bolster additional capabilities to our product offerings.

Key Business Metrics

We monitor the following key metrics to measure our performance, identify trends, formulate business plans and make strategic decisions.

Recurring Software Customers

We believe that our ability to increase the number of subscription and other recurring contract type customers on our platform is an indicator of our market penetration, the growth of our business, and our potential future business opportunities. We have a history of growing the number of customers who have contracted for our IronDefense and IronDome platforms on a recurring basis, which does not include customers of professional service revenue. We have consistently increased the number of such customers period-over-period, and we expect this trend to continue as we increase subscription offerings to small and medium-sized businesses, in addition to increased subscription offerings for our larger enterprise customers. The following table sets forth the number of recurring software customers as of the dates presented:

	Year Ended January 31,	
	2021	2020
Recurring Software Customers	27	20
Year-over-year growth	35%	43%

Annual Recurring Revenue ("ARR")

ARR is calculated at a particular measurement date as the annualized value of our then existing customer subscription contracts and the portions of other software and product contracts that are to be recognized over the course of the contracts and that are designed to renew, assuming any contract that expires during the 12 months following the measurement date is renewed on its existing terms. The following table sets forth our ARR as of the dates presented:

	Year Ended January 31,	
	2021	2020
	(in millions)	
ARR	$25.8	$15.0
Year-over-year growth	72%	37%

Dollar-based Average Contract Length

Our dollar-based average contract length is calculated from a set of customers against the same metric as of a prior period end. Because many of our customers have similar buying patterns and the average term of our contracts is more than 12 months, this metric provides a means of assessing the degree of built-in revenue repetition that exists across our customer base.

We calculate our dollar-based average contract length as follows:

- Numerator: We multiply the average length of the contracts, measured in years or fractions thereof, by the respective revenue recognized for the last three months of each reporting period.

- Denominator: We use the revenue attributable to software and product customers for the same three month period used in the numerator. This effectively represents the revenue base that is being generated by those customers.

Dollar-based average contract length is obtained by dividing the Numerator by the Denominator. Our dollar-based average contract length decreased from 3.5 to 2.9 years, or 17%, as of January 31, 2021 as compared to January 31, 2020. As our revenues and our customer base increases, we expect our average contract length to trend downward over time. Declines in average contract length are not reflective of the average lifetime of a customer.

	Year Ended January 31,	
	2021	2020
	(in years)	
Dollar-based average contract length	2.9	3.5

Calculated Billings

Calculated billings is a non-GAAP financial measure that we believe is a key metric to measure our periodic performance. Calculated billings represent our total revenue plus the change in deferred revenue in a period. Calculated billings in any particular period aims to reflect amounts invoiced to customers to access our software-based, cybersecurity analytics products, cloud platform and professional services, together with related support services, for our new and existing customers. We typically invoice our customers on multi-year or annual contracts in advance, either annually or monthly. Calculated billings increased $19.7 million, or 85%, in fiscal 2021 over fiscal 2020. As calculated billings continues to grow in absolute terms, we expect our calculated billings growth rate to trend down over time. We also expect that calculated billings will be affected by timing of entering into agreements with customers; and the mix of billings in each reporting period as we typically invoice customers multi-year or annually in advance and, to a lesser extent, monthly in advance.

While we believe that calculated billings may be helpful to investors because it provides insight into the cash that will be generated from sales of our subscriptions, this metric may vary from period-to-period for a number of reasons, and therefore has a number of limitations as a quarter-to-quarter or year-over-year comparative measure. In addition, other companies, including companies in our industry, may calculate similarly-titled non-GAAP measures differently or may use other measures to evaluate their performance, all of which could reduce the usefulness of our metric of calculated billings as tools for comparison. Because of these and other limitations, you should consider calculated billings along with revenue and our other GAAP financial results.

The following table presents a reconciliation of revenue, the most directly comparable financial measure calculated in accordance with GAAP, to calculated billings:

	Year Ended January 31,		2021 vs 2020	
	2021	2020	Change in Dollars	Change in Percentage
	(in millions)			
Revenue	$29.2	$23.2	$ 6.0	26%
Add: Total Deferred revenue, end of period	34.0	20.3	13.7	67%
Less: Total Deferred revenue, beginning of period	20.3	20.3	0.0	0%
Calculated billings	42.9	23.2	19.7	85%

Components of Our Results of Operations

Revenue

Our revenues are derived from sales of software subscriptions, subscription-like software products and software support contracts as well as from professional services. These revenues accounted for 85% of our revenue for each of fiscal 2021 and fiscal 2020.

Our typical customer contracts and subscriptions range from one to five years. We typically invoice customers in advance. We combine intelligence dependent hardware and software licenses as well as subscription-type deliverables with the related threat intelligence and support and maintenance as a single performance obligation, as it delivers the essential functionality of our cybersecurity solution. Most companies also participate in the IronDome collective defense software solution that provides them access to IronNet's collective defense infrastructure linking participating stakeholders. As a result, we recognize revenue for this single performance obligation ratably over the expected term with the customer. Amounts that have been invoiced are recorded in deferred revenue or they are recorded in revenue if the revenue recognition criteria have been met. Significant judgement is required for the assessment of material rights relating to renewal options associated with our contracts.

Professional services revenues are generally sold separately from our products and include services such as development of national cyber security strategies, cyber operations monitoring, security, training, red team, incident response and tailored maturity assessments. Revenue derived from these services is recognized as the services are delivered.

Cost of Revenue

Cost of product, subscription and support revenue includes expenses related to our hosted security software, employee-related costs of our customer facing support, such as salaries, bonuses and benefits, an allocated portion of administrative costs and the amortization of deferred costs.

Cost of services revenue consists primarily of employee-related costs, such as salaries, bonuses and benefits, cost of contractors and an allocated portion of administrative costs.

Gross Profit

Gross profit, calculated as total revenue less total costs of revenue is affected by various factors, including the timing of our acquisition of new customers, renewals from existing customers, the data center and bandwidth costs associated with operating our cloud platform, the extent to which we expand our customer support organization, and the extent to which we can increase the efficiency of our technology and infrastructure through technological improvements. Also, we view our professional services in the context of our larger business and as a significant lead generator for future product sales. Because of these factors, our services revenue and gross profit may fluctuate over time.

Operating Expenses

Research and development

Our research and development efforts are aimed at continuing to develop and refine our products, including adding new features and modules, increasing their functionality, and enhancing the usability of our platform. Research and development costs primarily include personnel-related costs and acquired software costs. Research and development costs are expensed as incurred.

Sales and marketing

Sales and marketing expenses consist primarily of employee compensation and related expenses, including salaries, bonuses and benefits for our sales and marketing employees, sales commissions that are recognized as expenses over the period of benefit, marketing programs, travel and entertainment expenses, and allocated overhead costs. We capitalize our sales commissions and recognize them as expenses over the estimated period of benefit.

We intend to continue to make significant investments in our sales and marketing organization to drive additional revenue, further penetrate the market and expand our global customer base. In particular, we will continue to invest in growing and training our sales force, broadening our brand awareness and expanding and deepening our channel partner relationships. We expect our sales and marketing expenses to decrease as a percentage of our revenue over the long term, although our sales and marketing expenses may fluctuate as a percentage of our revenue from period to period due to the timing and extent of these expenses.

General and administrative

General and administrative costs include salaries, stock-based compensation expenses, and benefits for personnel involved in our executive, finance, legal, people and culture, and administrative functions, as well as third-party professional services and fees, and overhead expenses.

We expect that general and administrative expenses will increase in absolute dollars as we hire additional personnel and enhance our systems, processes, and controls to support the growth in our business as well as our increased compliance and reporting requirements as a public company.

Other income (expense), net

Other income (expense), net consists primarily of interest income, interest expense, and foreign currency exchange gains and losses.

Provision for income taxes

Provision for income taxes consists of federal and state income taxes in the United States and income taxes and withholding taxes in certain foreign jurisdictions in which we conduct business. We maintain a full valuation allowance on our U.S. federal and state deferred tax assets.

Results of Operations

Comparison of Fiscal 2021 and Fiscal 2020

The following tables set forth our consolidated statements of operations in dollar amounts and as a percentage of total revenue for each period presented (dollars in millions):

	Year Ended January 31,				2021 vs 2020	
	2021	Percentage of Revenue	2020	Percentage of Revenue	Change in Dollars	Change in Percentage
Software, subscription and support revenue	$ 24.7	85%	$ 19.8	85%	$ 4.9	25%
Professional services revenue	4.5	15%	3.4	15%	1.1	32%
Total revenue	29.2	100%	23.2	100%	6.0	26%
Cost of product, subscription and support revenue	5.4	18%	5.9	25%	(0.5)	(8)%
Cost of service revenue	1.6	5%	0.7	3%	0.9	129%
Total cost of revenue	7.0	24%	6.6	28%	0.4	6%
Gross profit	22.2	76%	16.6	72%	5.6	34%
Operating expenses:						
Research and development	25.8	88%	26.6	115%	(0.8)	(3)%
Sales and marketing	30.4	104%	17.9	77%	12.5	70%
General and administrative	21.3	73%	20.5	88%	0.8	4%
Total operating expenses	77.5	265%	65.0	280%	12.5	19%
Operating loss	(55.3)	(189)%	(48.4)	(209)%	(6.9)	14%
Other income, net	(0.0)	0%	0.5	2%	(0.5)	(100)%
Loss before provision for income taxes	(55.3)	(189)%	(47.9)	(206)%	(7.4)	15%
Provision for income taxes	(0.1)	(0)%	(0.0)	(0)%	(0.1)	NM
Net loss	$(55.4)	(190)%	$(47.9)	(206)%	$ (7.5)	16%

Revenue

Total revenue increased by $6.0 million or 26% in fiscal 2021 compared to fiscal 2020 due to expansion of sales in all geographies and industries. Products, subscription and support revenue accounted for 85% of our total revenue in both fiscal 2021 and fiscal 2020. Subscription revenue increased by $6.0 million or 154%, in fiscal 2021, from $3.9 million to $9.9 million and accounted for 40% of our total Software revenue in fiscal 2021 up from 20% in fiscal 2020.

Professional services revenue increased $1.1 million or 32% in fiscal 2021 compared to fiscal 2020 and accounted for 15% of our total revenue in both fiscal 2021 and fiscal 2020.

Cost of revenue

Total cost of revenue increased by $0.4 million or 6%, in fiscal 2021, compared to fiscal 2020. Cost of product, subscription and support revenue decreased by $0.5 million or (8)%, in fiscal 2021, compared to fiscal 2020. The decrease was due primarily to more efficient purchasing of third-party computing costs and increased efficiency in providing software support to customers.

Cost of service revenue increased by $0.9 million in fiscal 2021, compared to fiscal 2020. The increase in cost of service revenue was primarily due to an increase in overall professional services activity in fiscal 2021

compared to fiscal 2020 combined with an increasing proportion of traditional services margin contracts in the mix, resulting in a decline in the overall services margin to 64%.

Gross Profit and Gross Margin

Favorable changes in the cost of revenue resulted in an increase in software gross margin to 78.1% in fiscal 2021 compared to 70.2% in fiscal 2020. We expect that gross margins for fiscal 2022 will continue to be above the fiscal 2020 level. However, margins may remain volatile compared to fiscal 2021 due to the continuing presence of large contracts in our revenue mix.

The following tables show gross profit and gross margin, respectively, for software products and support revenue and professional services revenue for fiscal 2021 as compared to fiscal 2020.

	Year Ended January 31,		2021 vs 2020	
	2021	2020	Change in Dollars	Change in Percentage
	(in millions)			
Software products	$19.3	$13.9	$ 5.4	39%
Professional services	2.9	2.6	0.3	12%
Total gross profit	22.2	16.5	5.7	35%

	2021	2020	Change
Software products	78.1%	70.2%	7.9%
Professional services	64.4%	79.4%	(15.0)%
Total gross margin	76.0%	71.6%	4.4%

Operating expenses

Research and development

Research and development expenses decreased by $0.8 million or (3%), in fiscal 2021, compared to fiscal 2020 as we reorganized our engineering departments towards our cloud-based and increasingly SaaS-delivered software offerings and paused net hiring as we completed that transition. At 88% of total revenues in fiscal year 2021 compared to 115% in fiscal 2020, we expect that our overall R&D expenditure rate as a percentage of sales will continue to decline in the future.

Sales and marketing

Sales and marketing cost increased by $12.5 million or 70% in fiscal 2021, compared to fiscal 2020, primarily due to the continued build out of our sales force globally. We either expanded or initiated activity in Singapore, Japan, Australia, the United Kingdom and in the United Arab Emirates throughout fiscal 2020, resulting in a partial year impact to sale and marketing costs. At 104% of total revenues in fiscal 2021 compared to 77% in fiscal 2020, we expect that our overall sales and marketing expenditure rates as a percentage of revenues will begin to decline in the future.

General and administrative

General and administrative costs increased by $0.8 million or 4% in fiscal 2021, compared to fiscal 2020 primarily due to $1.5 million of one-time charges relating to our response to COVID-19 restrictions and our staffing shift towards our cloud deployment and support models. These one-time charges included the costs of ending or reducing existing office leases, and severance and extended health benefits for employees. Absent those charges, general and administrative costs would have declined by $0.6 million, or (3%). At 68% of total revenues in fiscal 2021 compared to 88% in fiscal 2020, excluding the one-time charges, we expect that our overall general and administrative expenditure rates as a percentage of revenues will continue to decline in the future.

BENEFICIAL OWNERSHIP OF SECURITIES

Security Ownership of Certain Beneficial Owners and Management of LGL

The following table sets forth information regarding the beneficial ownership of LGL common stock as of (i) March 15, 2021 (prior to the Business Combination and the Private Placement) and (ii) immediately following the consummation of the Business Combination by:

- each person known by LGL to be the beneficial owner of more than 5% of LGL's outstanding shares of common stock either on the LGL Record Date or after the consummation of the Business Combination;
- each of LGL's current executive officers and directors that beneficially owns any shares of LGL common stock;
- all of LGL's current executive officers and directors as a group;
- each person who will become a named executive officer or a director of the Combined Company upon the consummation of the Business Combination; and
- all of the Combined Company's executive officers and directors as a group immediately following the consummation of the Business Combination.

At any time prior to the special meeting, during a period when they are not then aware of any material nonpublic information regarding LGL or its securities, the Sponsor, LGL's officers and directors, IronNet or IronNet stockholders and/or their respective affiliates may purchase shares from institutional and other investors who vote, or indicate an intention to vote, against the Business Combination proposal, or execute agreements to purchase shares from such investors in the future, or they may enter into transactions with such investors and others to provide them with incentives to acquire shares of LGL common stock or vote their shares in favor of the Business Combination proposal and the other proposals to be presented at the special meeting. The purpose of such share purchases and other transactions would be to increase the likelihood of satisfaction of the voting requirements for each of the proposals to be presented at the special meeting and to help ensure that LGL has in excess of the required dollar amount to consummate the Business Combination under the Merger Agreement, where it appears that such requirements would otherwise not be met. While the exact nature of any such incentives has not been determined as of the date of this proxy statement/prospectus, they might include, without limitation, arrangements to protect such investors or holders against potential loss in value of their shares, including the granting of put options and the transfer to such investors or holders of shares or warrants owned by the LGL initial stockholders for nominal value.

In addition, with the agreement of IronNet, LGL may seek to accomplish the Business Combination with IronNet through the use of a tender offer that conforms to the requirements of LGL's amended and restated certificate of incorporation and otherwise complies with applicable tender offer regulations. The identity of the bidder and the terms of any such tender offer would be determined at that time. In such instance, that number of shares acquired coupled with the shares of the Sponsor and affiliates and associates of Sponsor may have sufficient voting power to approve a second step merger to effectuate a complete acquisition of IronNet.

Entering into any such arrangements may have a depressive effect on LGL common stock. For example, as a result of these arrangements, an investor or holder may have the ability to effectively purchase shares at a price lower than market and may therefore be more likely to sell the shares it owns, either prior to or immediately after the special meeting.

As of the date of this proxy statement/prospectus, no agreements dealing with the above have been entered into. LGL will file a Current Report on Form 8-K to disclose any arrangements entered into or significant purchases made by any of the aforementioned persons that would affect the vote on the Business Combination proposal and the other proposals or the number of shares that will be redeemed. Any such report will include descriptions of any arrangements entered into or significant purchases by any of the aforementioned persons.

	Before the Business Combination(1)		After the Business Combination(2)	
Name and Address of Beneficial Owner	Amount and Nature of Beneficial Ownership	Approximate Percentage of Outstanding Shares	Amount and Nature of Beneficial Ownership	Approximate percentage of Outstanding Shares
Directors and Executive Officers Pre-Business Combination(3)				
All executive officers and directors as a group (seven individuals)	—	—	—	—
Directors and Named Executive Officers Post-Business Combination(4)				
Gen. Keith B. Alexander (Ret.)(5)	—	—	17,739,548	17.8%
William E. Welch	—	—	—	—
Sean Foster	—	—	—	—
Donald R. Dixon(6)	—	—	9,926,315	10.0%
Mary E. Gallagher	—	—	—	—
Vadm. John M. McConnell (Ret.)	—	—	242,268	*
Gen. John M. Keane (Ret.)	—	—	242,268	*
André Pienaar(7)	—	—	6,646,604	6.7%
Hon. Michael J. Rogers	—	—	242,268	*
Theodore E. Schlein(8)	—	—	5,675,407	5.7%
Vadm. Jan E. Tighe (Ret.)	—	—	—	—
Robert LaPenta Jr.	—	—	—	—
All executive officers and directors as a group (15 individuals)(9)	—	—	40,795,434	37.7%
Five Percent Holders				
LGL Systems Acquisition Holding Company, LLC	4,312,500(10)(11)	20.0%	3,800,375(4)(5)	3.2%
LGL Systems Nevada Management Partners LLC	4,312,500(10)(11)	20.0%	3,800,375(4)(5)	3.2%
BlueCrest Capital Management Limited(12)	1,160,000	5.4%	1,160,000	*
Glazer Capital, LLC(13)	1,107,047	5.1%	1,107,047	*
Entities affiliated with ForgePoint Capital(6)	—	—	9,684,047	9.5%
C5 Partners, LLC(7)	—	—	6,646,604	6.5%

* Less than 1%.

(1) The pre-Business Combination percentage of beneficial ownership of LGL in the table below is calculated based on 17,250,000 shares of Class A common stock and 4,312,500 shares of Class B common stock outstanding as of the LGL Record Date. The amount of beneficial ownership does not reflect the common stock issuable upon exercise of LGL's warrants as such warrants may not be exercisable within 60 days. Unless otherwise indicated, LGL believes that all persons named in the table have sole voting and investment power with respect to all shares of LGL common stock beneficially owned by them prior to the Business Combination.

(2) The post-Business Combination "Amount and Nature of Beneficial Ownership" and "Approximate Percentage of Outstanding Shares" is calculated based on 119,324,375 shares of Combined Company Common Stock expected to be outstanding immediately following consummation of the Business Combination and assumes an exchange ratio for converting each share of IronNet common stock and

IronNet preferred stock (with each share of IronNet preferred stock being treated as if it were converted into ten shares of IronNet common stock on the effective date of the Business Combination) into shares of LGL common stock of approximately 0.8076 and excludes any Earnout Shares that may become payable. Such expected number of shares of LGL common stock outstanding amount (i) assumes that no Public Stockholders properly elect to redeem their shares for cash, (ii) includes the shares issued in the Private Placement and (iii) includes the shares of LGL common stock that will be issuable upon exercise of IronNet options and IronNet warrants following consummation of the Business Combination and that will become exercisable, and IronNet restricted stock units that will vest, within 60 days of March 15, 2021 and (iv) takes into account that the Sponsor that immediately prior to consummation of the Merger the Sponsor will automatically be deemed to transfer to LGL, surrender and forfeit for no consideration 25.0% (or 1,078,125) of its Founder Shares pursuant to the Sponsor Support Agreement. The amount of beneficial ownership for each individual or entity post-Business Combination does not include shares of common stock issuable upon exercise of (i) the Public Warrants included in the units offered in the Initial Public Offering, (ii) the Private Warrants or (iii) the shares of LGL common stock that will be issuable upon exercise of IronNet options and IronNet warrants or the vesting of IronNet restricted stock units following consummation of the Business Combination, in each case where such securities will not become exercisable or vest, as applicable, within 60 days of March 15, 2021. Unless otherwise indicated, LGL believes that all persons named in the table have sole voting and investment power with respect to all LGL common stock shown to be beneficially owned by them after giving effect to the Business Combination.

(3) Unless otherwise indicated, the business address of each of the individuals is LGL Systems Acquisition Corp., 165 W. Liberty St., Suite 220, Reno, NV 89501.

(4) Unless otherwise indicated, the business address of each of the individuals is IronNet Cybersecurity, Inc., 7900 Tysons One Place, Suite 400, McLean, Virginia 22102.

(5) Includes (a) 13,701,745 shares of Combined Company Common Stock to be held by Gen. Keith B. Alexander (Ret.), (b) 2,584,194 shares of Combined Company Common Stock to be held by the Keith B. Alexander Irrevocable Third-Generation Trust, and (c) 1,453,609 shares of Combined Company Common Stock to be held by the Keith B. Alexander Irrevocable Second-Generation Trust.

(6) Includes (a) 242,268 shares of Combined Company Common Stock to be held by Donald R. Dixon, (b) 4,447,632 shares of Combined Company Common Stock to be held by ForgePoint Cybersecurity Fund I, L.P., (c) 51,716 shares to be held by ForgePoint Affiliates Fund I, L.P., (d) 2,228,431 shares of Combined Company Common Stock to be held by ForgePoint Co-Investors I, L.P., (e) 742,204 shares of Combined Company Common Stock to be held by ForgePoint Co-Investors I-B, L.P., (f) 1,949,669 shares of Combined Company Common Stock to be held by ForgePoint Co-Investors I-C, L.P., and (g) 264,395 shares of Combined Company Common Stock to be held by ForgePoint Cyber Co-Investors I-E, L.P. Donald R. Dixon, one of IronNet's directors, is the general partner of each of the funds. Mr. Dixon and Alberto Yepez are the managing members of ForgePoint Cybersecurity Fund I, L.P., ForgePoint Cyber Affiliates Fund I, L.P., ForgePoint Co-Investors I, L.P., ForgePoint Co-Investors I-B, L.P., ForgePoint Co-Investors I-C, L.P., ForgePoint Co-Investors I-E, L.P. and exercise shared voting, investment and dispositive rights with respect to the shares of stock held by each of the funds. The address for all entities and individuals affiliated with ForgePoint Capital is 400 S El Camino Road, Suite 300, San Mateo, CA 94402.

(7) Andre Pienaar, one of IronNet's directors, William Kilmer and James Coats are the directors of C5 Investors General Partner Limited, who acts on behalf of C5 Investors LP the sole manager of C5 Partners LLC. C5 Capital Limited is the investment manager of C5 Investors LP and exercises voting, investment and dispositive rights with respect to the shares of stock held by C5 Partners, LLC. Andre Pienaar is the CEO and a director of C5 Capital Limited together with William Kilmer and Linda Zecher. The address of C5 Partners, LLC is 1209 Orange Street, City of Wilmington, 19801, County of New Castle, Delaware. The address of C5 Investors LP is P.O Box 309, Ugland House, Grand Cayman, KY1-110, Cayman Islands. The address of C5 Capital Limited is 7 Vigo Street, London, W1S 3HF, UK.

(8) Includes 5,534,660 shares of Combined Company Common Stock to be held by KPCB Digital Growth Fund II, LLC ("KPCB DGF II") and 140,747 shares of Combined Company Common Stock to be held by KPCB Digital Growth Founders Fund, LLC ("DGF II Founders"). All shares are held for convenience in the name of "KPCB Holdings, Inc., as nominee" for the accounts of such individuals and entities. The managing

member of KPCB DGF II is KPCB DGF II Associates, LLC ("DGF II Associates"). L. John Doerr, Theodore E. Schlein (who will be a director of the Combined Company) and Mary Meeker, the managing members of DGF II Associates, exercise shared voting and dispositive control over the shares held by KPCB DGF II. Such managing members disclaim beneficial ownership of all shares held by KPCB DGF II except to the extent of their pecuniary interest therein. The principal business address for all entities and individuals affiliated with Kleiner Perkins Caufield & Byers is c/o Kleiner Perkins Caufield & Byers, LLC, 2750 Sand Hill Road, Menlo Park, CA 94025.

(9) Includes (a) 40,714,678 shares of Combined Company Common Stock and (2) 80,756 shares of Combined Company Common Stock underlying options that are exercisable within 60 days of March 15, 2021.

(10) Represents shares of Class B common Stock held by LGL Systems Acquisition Holding Company, LLC (the Sponsor), of which LGL Systems Nevada Management Partners LLC is the managing member, after giving effect to the forfeiture of 1,078,125 shares pursuant to the Sponsor Support Agreement. LGL Systems Nevada Management Partners LLC appointed Marc J. Gabelli, Robert LaPenta Sr., Robert LaPenta Jr., Timothy J. Foufas, and Jeffrey M. Illustrato (appointed by Mr. Gabelli) as managers to approve actions of our sponsor. Each manager has one vote, and the approval of three of the five managers is required for approval of an action of the sponsor. Under the so-called "rule of three", if voting and dispositive decisions regarding an entity's securities are made by three or more individuals, and a voting or dispositive decision requires the approval of a majority of those individuals, then none of the individuals is deemed a beneficial owner of the entity's securities. Based on the foregoing, no individual manager exercises voting or dipositive control over any of the securities held by the Sponsor, even those in which he has a pecuniary interest. Accordingly, none of them are deemed to have or share beneficial ownership of the securities held by the Sponsor.

(11) Interests shown consist solely of Founder Shares, classified as Class B common stock. Such shares will automatically convert into Class A common stock at the time of LGL's initial business combination on a one-for-one basis, subject to adjustment.

(12) Represents shares held by BlueCrest Capital Management Limited, which serves as investment manager to Millais Limited, a Cayman Islands exempted company. Michael Platt is the principal, director and control person of BlueCrest. Based solely on information contained in a Schedule 13G/A filed with the Securities and Exchange Commission on February 12, 2021.

(13) Represents shares held by certain funds and managed accounts to which Glazer Capital serves as investment manager. Paul Glazer is the managing member of Glazer Capital. Based solely on information contained in a Schedule 13G filed with the Securities and Exchange Commission on February 16, 2021.

Table of Contents

SIGNATURES

Pursuant to the requirements of the Securities Act, the registrant has duly caused this registration statement to be signed on its behalf by the undersigned, thereunto duly authorized, in New York, NY, on the 14th day of May, 2021.

LGL SYSTEMS ACQUISITION CORP.

By: /s/ Robert LaPenta Jr.
Robert LaPenta Jr.
Co-Chief Executive Officer

POWER OF ATTORNEY

KNOW ALL MEN BY THESE PRESENTS, that each person whose signature appears below constitutes and appoints each of Robert LaPenta Jr. and Marc J. Gabelli as his true and lawful attorney-in-fact, with full power of substitution and resubstitution for him and in his name, place and stead, in any and all capacities to sign any and all amendments including post-effective amendments to this proxy statement/prospectus and to file the same, with all exhibits thereto, and other documents in connection therewith, with the Securities and Exchange Commission, hereby ratifying and confirming all that said attorney-in-fact or his substitute, each acting alone, may lawfully do or cause to be done by virtue thereof.

Pursuant to the requirements of the Securities Act of 1933, this registration statement has been signed by the following persons in the capacities and on the dates indicated.

Name	Title	Date
/s/ Marc J. Gabelli Marc J. Gabelli	Chairman and Co-Chief Executive Officer (Co-Principal Executive Officer)	May 14, 2021
/s/ Robert LaPenta Jr. Robert LaPenta, Jr.	Co-Chief Executive Officer and Chief Financial Officer (Co-Principal Executive Officer and Principal Accounting and Financial Officer)	May 14, 2021
/s/ Mary E. Gallagher Mary E. Gallagher	Director	May 14, 2021
/s/ Michael Ferrantino Michael Ferrantino	Director	May 14, 2021
/s/ Michael Martin Michael Martin	Director	May 14, 2021